جرائم الحاسوب والانترنت

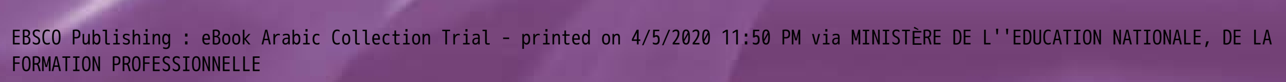
الدكتور علي جبار الحسيناوي
أستاذ القانون الجنائي المشارك
رئيس قسم القانون العام

الدكتور علي جبار الحسيناوي

جرائم الحاسوب والانترنت







جرائم الحاسوب والإنترنت

إعداد

د. علي جبار صالح الحسيناوي

أستاذ القانون الجنائي المشارك

رئيس قسم القانون العام

جامعة جدارا

1428هـ /2008م

بسم الله الرحمن الرحيم

﴿وإِمَّا تَخَافَنَّ مِنْ قَوْمٍ خِيَانَةً فَانبِذْ إِلَيْهِمْ عَلَى سَوَاءٍ إِنَّ اللهَ لا يُحِبُّ الْخَائِنِينَ﴾

[سورة الأنفال: الآية58]

الإهداء

إلى مَن رافقتني رحلة البذل والعطاء، وتوسّع عليّ

بالعون، والأمن، والقدرة والسعادة: زوجتي الكريمة

وأولادي

وإلى الأخ العزيز السيد حسين المجالي (أبو هزاع)

وإلى السيدة هيام جريسات (أم خليل)

المؤلف

شكر وتقدير

لابد من تقديم كلمة شكر وتقدير للأستاذ الدكتور هادي نهر/عميد كلية الدراسات اللغوية في جامعة جدارا لجهوده القيمة في مراجعة هذا المؤلف وتصحيح الأخطاء اللغوية فيه.

كما نسجل شكرنا وتقديرنا إلى السيد عمار الشريف/مدير مكتبة جامعة جدارا لما أبداه من مساعدة وتعاون في تهيئة المصادر اللازمة لإعداد هذا المؤلف.

ولا يسعنا أيضاً إلا أن نسجل شكرنا إلى الآنسة رانيا شوتر لجهودها في إعداد طبع هذا الكتاب.

وأخيراً نتقدم بشكرنا لكل من ساهم أو تعاون معنا في إنجاز هذا الجهد المتواضع ... ومن الله التوفيق.

المؤلف

المحتويات

المقدمة

تعد دراسة التطور التاريخي لجريمة الكمبيوتر والإنترنت تبعا لتطور التقنية واستخداماتها الخطوة الأولى لبيان سمات هذه الجريمة وطابعها الخاص كونها جرائم عابرة للحدود فلا ينحصر تأثيرها في الدولة التي تتم بها وقد تمتد آثارها لتصل إلى عدد غير محدود من الدول، وكون محل هذه الجريمة معطيات الكمبيوتر بدلالاتها الواسعة فهي جرائم ذات خصائص متفردة بها لا تتوفر في أي من الجرائم التقليدية في أسلوبها وطريقة ارتكابها.

تعد الستينات المرحلة الأولى من شيوع استخدام الكمبيوتر حيث ظهرت أول معالجات لجرائم الكمبيوتر كالمقالات والمواد الصحفية التي تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي والاستخدام غير المشروع للبيانات المخزنة في نظم الكمبيوتر وثار الجدل والتساؤل إن كانت مجرد سلوكيات غير أخلاقية أم هي جرائم بالمعنى القانوني ولكن بقي التعامل معها أقرب إلى النطاق الأخلاقي منه إلى النطاق القانوني، تزايد استخدام الكمبيوتر في السبعينات فظهرت الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر لتعالج العديد من الجرائم الفعلية وبدأ الحديث عنها بوصفها ظاهرة جرمية لا مجرد سلوكيات مرفوضة، إلى أن ظهر في الثمانينات مفهوم جديد لجرائم الكمبيوتر متعلقا بعمليات اقتحام نظم الكمبيوتر عن بعد، والفيروسات الإلكترونية والتي تقوم بعمليات تدميرية للملفات أو البرامج، وشاع الهاكرز وبدأت عملية تحديد سمات مرتكبي جرائم الحاسوب والإنترنت وظهر مصطلح (المجرم المعلوماتي).

شهدت التسعينات تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها، وأحدثت شبكة الإنترنت تسهيلات لعمليات دخول الأنظمة واقتحام شبكات المعلومات، فأصبحت تضم ملايين المستخدمين في كافة المدن حول العالم وشكلت بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات، وفي البداية لم يكن ثمة اهتمام بمسائل الأمن بقدر

ما كان الاهتمام ببناء الشبكة وتوسيع نشاطها، ولهذا لم يتم بناء الشبكة في المراحل الأولى على نحو يراعي تحديات أمن المعلومات، فالاهتمام الأساسي تركز على الربط والدخول ولم يكن الأمن من الموضوعات المهمة في بناء الشبكة.

ولكن بعد حادثة موريس تغيرت تماما هذه النظرة فقد استطاع الشاب موريس في 2\11\1988أن ينشر فيروس إلكتروني تمكن من مهاجمة آلاف الكمبيوترات عبر الإنترنت تسبب بأضرار بالغة أبرزها وقف آلاف الأنظمة عن العمل وتعطيل وإنكار الخدمة وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي 100000000 مائة مليون دولار ، وفي 1995 نجح هجوم مخطط له عرف باسم IP-SPOOFING أدى لوقف عمل الكمبيوترات الصحيحة على الخط وشغل كمبيوترات وهمية على أنها الكمبيوترات الموثوقة، وفي قضية الجحيم العالمي تمكنت هذه المجموعة من اختراق مواقع البيت الأبيض والجيش الأمريكي ووزارة الداخلية الأمريكية والشركة الفدرالية الأمريكية، كما انخرطت جهات تطبيق القانون وتنفيذه في العديد من الدول في تحقيق واسع حول إطلاق فيروس ميلسا 1999، وفي حادثة أخرى تمكن أحد الهاكرز (الإسرائيليين) من اختراق أنظمة معلومات حساسة في الولايات المتحدة الأمريكية والكيان الصهيوني 1998، وفي 1996 وبعد 20 يوما من فصله من العمل قام رئيس سابق لشركة اوميغا بإطلاق قنبلة إلكترونية ألغت كافة التصاميم وبرامج الإنتاج لأحد كبرى مصانع التقنية العالية وألحق خسائر بلغت 10مليون دولار.

بدأت مجتمعاتنا العربية بالتأثر بشكل ملموس بمخاطر هذا النمط المستجد من الإجرام عبر هذه التقنية التي من الممكن أن يكون خطرها المحتمل في البيئة العربية كبيرا باعتبار أن الجاهزية التقنية والتشريعية والادائية لمواجهتها ليست بالمستوى المطلوب إن لم تكن غائبة تماما، وبالمقابل تعتبر جرائم الكمبيوتر والإنترنت من أخطر الجرائم التي تقترف في الدول المتقدمة فقد تزايدت نتيجة لذلك خطط مكافحتها وانصبت الجهود على دراستها المتعمقة وخلق آليات قانونية للحماية من أخطارها، وبرز في هذا المجال المنظمات الدولية والإقليمية، وإدراكا لقصور القوانين الجنائية بما تتضمنه من نصوص التجريم التقليدية كان لا بد للعديد من الدول من وضع قوانين

وتشريعات خاصة، أو العمل على تعديل قوانينها الداخلية لضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم.

تكمن أهمية هذه الدراسة في الأهداف التي تسعى إلى الوصول إليها، وذلك بالتعرف على جرائم الانترنت والكمبيوتر والخصائص المتفردة بها والتي لا تتوافر في أي من الجرائم التقليدية في اسلوبها وطريقة ارتكابها حيث يكون الحاسب الآلي هو آداة إرتكاب الجريمة كما وترتكب هذه الجرائم عبر شبكة الانترنت ويتمتع مرتكب هذه الجريمة بخبرة فائقة في مجال الحاسب الآلي ويمارس جريمته على معطيات الحاسوب إما بذاتها أو بما تمثله.

حيث أدى الانتشار الواسع للإنترنت والكمبيوتر والتطور الهائل في عالم البرمجيات وتزايد الاعتماد على بنوك المعلومات والكمبيوتر في نواحي الحياة كافة إلى وصول هذه التقنية العالية إلى أيدي الخير والشر معا حيث استغل البعض معرفتهم بالتقنية العالية لارتكاب الجرائم سواء الواقعة على المعلومات أو التي ترتكب بواسطة المعلوماتية، كما أن هذه الجريمة لا حدود جغرافية لها مما يكسبها طابعا دوليا وتعد هذه السمة نقطة هامة تستحق الوقوف عندها وبحثها باستفاضة باعتبار جرائم الانترنت من الجرائم العابرة للحدود وترجع تسميتها بالعالمية إلى مزاولة الأنشطة الإجرامية فيها على مستوى عالمي وعبر الدول والحدود نتيجة للتقدم المذهل في وسائل الاتصالات والمواصلات ولكنها في حقيقتها تعتبر من الجرائم الداخلية التي يعاقب عليها قانون العقوبات الوطني.

تهدف هذه الدراسة لتوضيح جرائم الإنترنت مع الأخذ بعين الاعتبار للخصوصية التي تتمتع بها كون محلها دائما هو معطيات الحاسوب من بيانات مدخلة ومعلومات معالجة ومخزنة وكذلك البرامج بأنواعها وصولا إلى المعلومات المستخرجة والمتبادلة بين النظم، من ثم سنبين مدى فعالية الجهود المبذولة لمواجهة هذا النوع من الجرائم إبتداءا من مرحلة التحقيق ووصولا لمرحلة الإثبات موضحين مواقع القصور والإشكال في بيئة الحاسوب في كلتا المرحلتين.

كما وتهدف الدراسة لبيان أوجه القصور التشريعي الوطني عن مواكبة مثل هذه الجرائم سريعة التطور وذلك سعيا للتوصل لآليات قادرة على احتوائها ومواجهتها نظرا لطبيعتها العالمية

كونها جرائم عابرة للحدود فمن الضروري التطرق للجهود الدولية المبذولة لمواجهتها، فالتعرف على ماهية هذه الجرائم وآثارها وطرق مكافحتها الدولية والوطنية يعد الهدف الأبرز لهذه الدراسة كمحاولة للوصول إلى الآلية المثلى للتعاطي مع هذه الجرائم.

تم تقسيم الدراسة إلى خمسة فصول تناول الأول منها جرائم الحاسوب والانترنت حيث تم التعريف بها عبر التطور التاريخي لتقنية الحاسوب والإنترنت وذلك ببيان ماهية الحاسوب ومكوناته وكذلك ماهية الانترنت في مبحث أول، وتم تناول جرائم الحاسوب في مبحث ثان من حيث مفهومها والطبيعة القانونية لها وصولا إلى جرائم الإنترنت في مبحث ثالث من حيث مفهومها وطبيعتها القانونية والتعرف على وسطاء خدمة الانترنت.

أما جرائم الحاسوب فقد تم التطرق إليها في الفصل الثاني من هذه الدراسة بتقسيمها إلى قسمين حيث احتوى القسم الأول على الجرائم الواقعة على الحاسوب وتم تناول جرائم الاعتداء على حقوق المؤلف ومن ثم سرقة منفعة الحاسوب وكذلك تزوير واتلاف مكونات الحاسوب، واحتوى القسم الثاني منها على الجرائم الواقعة بواسطة الحاسوب كجريمة الاستغلال غير المشروع لبطاقات الإئتمان، وتناول الفصل الثالث جرائم الانترنت حيث تم تقسيمها كذلك إلى جرائم الاعتداء على الأشخاص عبر الانترنت كجريمة القدح والذم والتحقير وجريمة إفساد الأخلاق والاستغلال الجنسي للأطفال عبر الانترنت، أما جرائم الاعتداء على الأموال عبر الانترنت فتم تناول جريمة التحويل الإلكتروني غير المشروع للأموال وجريمة إتلاف نظم المعلومات كأمثلة على هذه الأنواع من الجرائم.

وتناول الفصل الرابع التحقيق والإثبات في جرائم الحاسوب والانترنت عبر ثلاثة مباحث تناول الأول منها الجهات المختصة بالتحقيق في جرائم الحاسوب والإنترنت ومن ثم إجراءات التحقيق الفني في جرائم الحاسوب والانترنت والتي تم تناولها من خلال المبحث الثاني لهذه الدراسة وصولا إلى الإثبات الجنائي لهذة الجرائم والمشكلات التي يواجهها في بيئة الحاسوب والانترنت، وتطرق الفصل الخامس من هذه الدراسة للجهود العربية والدولية المبذولة لمواجهة جرائم الحاسوب والانترنت عبر أربعة مباحث احتوى الأول منها على الجهود الدولية لمواجهة

جرائم الحاسوب والانترنت ومن ثم الجهود العربية المبذولة في هذا السياق وتم التطرق لبعض التشريعات الوطنية العربية منها والأجنبية لمواجهة جرائم الانترنت.

الفصل الأول

جرائم الحاسوب والانترنت

يعتمد الانترنت في وجوده على تقنية الحاسوب، وبما أن ارتباط الحاسوب بالإنترنت أمر لابد منه سيتم في هذا الفصل التعريف بكل من الحاسوب والانترنت وبيان ماهية جرائم الحاسوب وجرائم الانترنت بغرض التمييز ما بينها بالرغم من الارتباط الوثيق ما بين الانترنت والحاسوب.

إن هذه التقنية الحديثة في التحكم بالمعلومات واعتبار الانترنت سيل المعلومات المتدفق تعد آداة رفيعة المستوى لارتكاب الجريمة حيث يضعف في هذه البيئة الامن والتحكم والمراقبة مما يؤدي بصعوبة اكتشاف هذه الجرائم.

المبحث الأول

التعريف بالحاسوب والانترنت

تعد دراسة التطور التاريخي لهذه التقنية المعلوماتية السبيل لبيان ماهية الحاسوب ومكوناته وماهية الانترنت، وسيتم تقسيم هذا المبحث إلى ثلاثة مطالب حيث يتناول الأول منها التطور التاريخي لتقنية الحاسوب والانترنت، ومن ثم سيتم استعراض ماهية الحاسوب ومكوناته في مطلب ثان، وماهية الانترنت سيتم تناولها في المطلب الثالث.

المطلب الأول

التطور التاريخي لتقنية الحاسوب والإنترنت

الحاسوب عبارة عن جهاز إلكتروني رقمي متعدد الوظائف يقوم باستقبال البيانات ومعالجتها وتخزينها للحصول على معلومات[1]، تعد بدايات صناعة الحواسيب وانطلاق ثورة الالكترونيات مستقلة عن وسائل الاتصال والتي وقعت في اربعينيات القرن الماضي حيث اقتصر استخدام الحواسيب على المؤسسة العسكرية وفي مجالات ضيقة لدى المؤسسات الكبرى التابعة للدولة، كما بدأ الاستخدام التجاري للحواسيب في الخمسينات وفي ذلك الوقت لم يكن في الأذهان تصور للخطر الناجم عن استخدامها وإن وجد فلم يتعلق بالإجرام بل في البطالة التي قد تنجم عنها في قطاع الانتاج ومخاطرها على سوق العمل في الدولة[2]. بدأت ظاهرة "جرائم الحاسوب" بالظهور في نهاية الخمسينيات من القرن العشرين ، ولكن ضمن إطار مفهوم "إساءة استخدام الحاسوب " المؤسس على البعد الأخلاقي[3].

إن ثورة المعلومات والثورة الجديدة في عالم الاتصال ونقل المعلومات أتاحت للأفراد والمؤسسات فرصة الولوج إلى بنوك وقواعد المعلومات على الصعيدين المحلي و الدولي، فانعكس هذا الأمر إيجاباً على القطاعات الاقتصادية وصار مصدراً غنياً بالمعلومات لمراكز اتخاذ القرار [4].

([1]) فراس محمد العزة وآخرون، مهارات الحاسوب- الحاسوب والبرمجيات الجاهزة، دار اليازوري العلمية للنشر والتوزيع، عمان، ط1، 2003، ص13.

([2]) يونس عرب، موسوعة القانون وتقنية المعلومات، دليل امن المعلومات والخصوصية- جرائم الكمبيوتر والانترنت، منشورات اتحاد المصارف العربية، الجزء الأول، ط1، 2002، ص299.

([3]) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط، 3من 1-3 مايو 2000.

([4]) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول، 2004، ط3، من 1-3 مايو 2000.

تزايد انتشار الحواسيب في الخمسينات وتعددت استخداماتها وبدأت بالظهور جرائم الحاسوب الوليدة آنذاك وكان الخطر الناجم عن العبث في الحواسيب محدودا في ذلك الوقت لقلة استخدام الحاسوب، ارتكبت أول جريمة بواسطة الحاسوب عام 1958 وبدأ رصد ونشرما تتوافر بشأنه تقارير من حالات إساءة استخدام الحاسوب في أمريكا حيث صنفت إلى جرائم العبث أو التخريب الموجه إلى الحاسوب، سرقة المعلومات أو الممتلكات، الاحتيا ل أو الغش المالي، والاستخدام غير المصرح به لخدمات الحاسوب[5]. وكانت الانشطة الجرمية المتصلة بالحاسوب تصاغ وفق مدلول أخلاقي أكثر منه قانوني مما أدى لعدم التمييز بين الأنشطة الجرمية التي تستهدف ماديات الحاسوب وتلك التي تستهدق معطيات الحاسوب وحتى الرؤية القانونية تعاملت مع المكونات كممتلكات مادية منقولة لاعتداءات جرمية لها ذات الدلالة للجرائم التقليدية سواء الاتلاف أو السرقة أو الاحتيال.

وبدأ بروز مفهوم اساءة استخدام الكمبيوتر والعبث بالبيانات في مطلع الستينات وتطور إلى مفهوم جريمة السيبر التي لا تحدها حدود ولا تقف في مواجهتها قيود بل إلى نمط جديد من حروب المعلومات والإرهاب الالكتروني في الوقت الحاضر وبين هاتين النقطتين ثمة تغيرات وتطورات وأحداث تقدم الدليل على التطور المتسارع لظاهرة جرائم الكمبيوتر على نحو يوازي التطور الهائل في تقنية المعلومات ذاتها[6]. وحتى عقد الستينات اتسعت دائرة تناول أنشطة إساءة استخدام الحاسوب عبر وسائل الإعلام حتى وصفت هذه المرحلة بأنها مرحلة طرح البيانات الأولية لأجرام تقنية المعلومات[7].

---

(5) يونس عرب، موسوعة القانون وتقنية المعلومات، دليل امن المعلومات والخصوصية- جرائم الكمبيوتر والانترنت، منشورات اتحاد المصارف العربية، الجزء الأول، ط1، 2002، ص300.

(6) يونس عرب، موسوعة القانون وتقنية المعلومات، دليل امن المعلومات والخصوصية- جرائم الكمبيوتر والانترنت، منشورات اتحاد المصارف العربية، الجزء الأول، ط1، 2002، ص299.

(7) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط، 3من 1-3 مايو 2000.

وبعد الاندماج مابين الحوسبة والاتصالات ظهرت الانشطة التي تستهدف المعطيات عن بعد كاختراق شبكات الحواسيب للتوصل غير المصرح به مع أنظمة الاتصال البعدي وفي السبعينات تم رصد 1600 حالة لإساءة استخدام الحاسوب حدثت منذ عام 1958 وتم تقديم استبيان من قبل معهد ستانفورد للتحضير لمناقشة مشروع قانون الجريمة الاقتصادية، أما معهد الاجرام وقانون العقوبات الاقتصادي في ألمانيا الاتحادية قام بتقديم دراسة تضمنت وصفا لـ 31 جريمة ارتكبت بواسطة الحاسوب، وتوالت الدراسات التي رصدت وسجلت العديد من جرائم الحاسوب[8].

وإذا كانت السبعينات قد حملت بذور ملامح ظاهرة جرائم الحاسوب"، فأن عقدي الثمانينات والتسعينات، قد جلبا تحديداً لمفهوم وماهية هذه الجرائم، فقد تبلور مفهوم ظاهرة جرائم الحاسوب، واتسعت ظاهرة الشعور بعظم وأهمية المعلومات وحجم المخاطر الناتجة عن الاعتداء عليها ووجوب حمايتها من خلال توفير أدوات قانونية فاعلة لوسائل معالجتها ونقلها[9]. كون تقنية المعلومات وتحديدا الانترنت أفرزت آثار شاملة على البناء الاداري والاقتصادي والسياسي والاجتماعي والثقافي والقانوني للدولة، وقد أثرت على مختلف مناحي النشاط الانساني[10].

وبنتيجة هذا التطور في عالم المعلوماتية نشأت ونمت أنواع جديدة من الجرائم التي ما كانت لتبصر النور لولا ظهور الكمبيوتر. حيث شهدت التسعينات والقرن الحالي أنواعاً فريدة من جرائم الكمبيوتر وترافق ذلك مع ظهور الانترنت وبدأت أنشطة الهاكرز باختراق مواقع المعلومات ونظمه عبر الانترنت، والدخول دون تصريح أو تخويل إلى النظم والعبث بالبيانات والمعلومات المخزنة فيه أو تدميرها التي يتيحها الانترنت بشكل كبير، وكذلك تعطيل الأنظمة بالبرمجيات

([8]) يونس عرب، موسوعة القانون وتقنية المعلومات، دليل امن المعلومات والخصوصية- جرائم الكمبيوتر والانترنت، منشورات اتحاد المصارف العربية، الجزء الأول، ط1، 2002، ص302

([9]) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000.

([10]) يوسف عراب، ورقة عمل – متطلبات ومخاطر الانفتاح الالكتروني من النواحي الفنية والتشريعية، الاردن، 2003، www.arablow.org

الخبيثة أو التدمير المادي لها أو استغلالها دون تصريح أو الهجوم عبر الانترنت على مواقع المعلوماتية لتعطيل عملها، وشملت جرائم الكمبيوتر أنشطة التجسس الصناعي والأمني والاستيلاء على البيانات ذات القيمة الاقتصادية أو الاستيلاء على أرقام بطاقات الائتمان واستخدامها بشكل غير مشروع للإستيلاء على المال، وكذلك الإساءة إلى سمعة الأفراد وتحقيرهم عبر الرسائل الإلكترونية، أو استغلال مواقع انترنت لترويج محتوى غير قانوني[11].

أصبحت هذه الجرائم اليوم تطرح إشكاليات خطيرة على الصعيدين الاقتصادي والقانوني، فهي تشكل خطراً على التوظيفات والاستثمارات الهائلة في قطاع المعلوماتية مما قد يحد من جدوى هذه الاستثمارات بسبب القرصنة مثلاُ، كما تستدعي مراجعة شاملة للأحكام والنصوص القانونية، هذه المراجعة تظهر دون عناء أن القوانين التقليدية قاصرة عن تغطية هذه الجرائم لأن تطبيق هذه القوانين يفترض وقوع الجرم على أموال مادية بينما جرائم المعلومات تقع على أموال معنوية لا تغطيها هذه القوانين[12].

إن هذه الجرائم فيها خطورة كبيرة على كافة دول العالم ومع انتشار هذه الجرائم وتزايدها وتزايد حجم الاضرار الناشئة عنها وأخطار الاعتداءات على البيانات الشخصية للدول وللمنظمات فترتب على ذلك إبرام اتفاقيات دولية في محاولة لترسيخ وجوب التعاون الدولي لمواجهة جرائم الكمبيوتر[13]، وعلى رأسها الأمم المتحدة والمجلس الأوروبي وبعض الهيئات الأخرى فكانت هي الاساس الذي ارتكزت عليه الاتفاقيات الدولية لمواجهة جرائم الانترنت والحاسوب.

ونشير في هذا المقام إلى أن هذه الجرائم الحديثة والمستحدثة تتنوع وتتضاعف يوماً بعد يوم، ويختلف مرتكبوها عادة عن المجرمين التقليديين لأنهم في الغالب أشخاص على مستوى

([11]) يونس عرب، موسوعة القانون وتقنية المعلومات، دليل امن المعلومات والخصوصية- جرائم الكمبيوتر والانترنت، منشورات اتحاد المصارف العربية، الجزء الأول، ط1، 2002، ص306.

([12]) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، المرجع السابق.

([13]) محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة، عمان- الاردن، ط1، 2004، ص74.

عال من العلم والمعرفة، هذا الوضع يجعلنا بطبيعة الحال نخرج عن الإطار التقليدي للنظرة إلى المجرم العادي[14].

[14] وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، المرجع السابق.

المطلب الثاني

ماهية الحاسوب ومكوناته

يعرف الحاسوب بأنه "الآلة المتفاعلة مع الأوامر الإنسانية ذات التقنية المتطورة في معالجة البيانات"[15]. ويُعرف كذلك بأنه "عبارة عن جهاز إلكتروني يتكون من مجموعة من الأجهزة أو الوحدات التي تعمل بصورة متكاملة مع بعضها بعضاً بهدف تشغيل مجموعة البيانات الداخلة طبقاً لبرنامج مُحدد تم وضعه مسبقاً للحصول على نتائج معينة[16].

وعرفه المشرع الامريكي بأنه "آداة إلكترونية مغناطيسية مرئية كهروكيميائية أو اية آداة ذات سرعة عالية في معالجة البيانات تؤدي عمليات منطقية رياضية أو عمليات تخزين وتتضمن أية تسهيلات لتخزين البيانات أو تسهيلات إتصالية ذات ارتباط مباشر ب/أو التشغيل"[17].

ويمكن تعريف الحاسوب أيضاً بأنه "نظام معالجة كهربائي سريع دقيق، يستخدم في تداول البيانات ومصمم لتقبل وتخزين هذه البيانات ومعالجتها وإعطاء النتائج تبعاً للبرنامج المخزن الذي يتألف بدوره من مجموعة أوامر موضحة خطوة خطوة"[18].

ويتكون الحاسوب من وحدة معالجة مركزية Central processing unit (CPU)، بالإضافة إلى ملحقاتها Peripherals يتم بواسطتها إدخال البيانات ثم معالجتها وإخراج المعلومات[19]، ويمتلك الحاسوب مزايا متعدّدة جعلته يتمتع بأهمية بالغة وتطبيقات لا حصر لها ومنها[20]:

([15]) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه في القانون الجنائي، جامعة عين شمس –كلية الحقوق، سنة 2004، ص55.

([16]) هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992– ص6.

([17]) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص57

([18]) محمد أحمد فكيرين، أساسيات الحاسوب، دار الراتب الجامعية، بيروت، 1993م، ص8.

([19]) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص54.

1. القدرة على تنفيذ التعليمات المخزونة بشكل تلقائي دون تأخير أو مساعدة الإنسان.

2. السرعة الهائلة التي يستطيع بها الحاسوب معالجة البيانات.

3. الدقة العالية في الحصول على النتائج الموثوقة بواسطة الحاسوب.

4. القدرة على تخزين البيانات واسترجاعها وقت الحاجة.

5. إمكانية استخدام الحاسوب في كل مجالات الحياة

ويقسم قانون الحاسوب وفق التقنية مكونات الحاسوب إلى ثلاثة أقسام وهي:

أولا: الكيان المادي للحاسوب hardware

وهي العناصر المادية التي يتركب منها نظام الحاسوب كلوحة المفاتيح والشاشة والطابعة ووحدة المعالجة المركزية[21]. ولكل منها وظيفة وتعمل مجتمعة كنظام متكامل كالآتي:

1. وحدات الإدخال: وهي مجموعة الوحدات المسؤولة عن إيصال البيانات للحاسوب[22]، فتقوم باستقبال البيانات المدخلة إلى الحاسوب وتمريرها داخل الجهاز إلى وحدة الذاكرة للتخزين ومن أجهزة الإدخال لوحة المفاتيح،الماسح، الفأرة، مشغل الاقراص.

2. وحدة الذاكرة: وتقوم هذه الوحدة بتخزين البرامج والبيانات. وهذه الوحدة على صنفين[23]:

أ. وحدة الذاكرة الرئيسية أو العشوائية: وتسمى كذلك ذاكرة القراءة والكتابة وتستخدم لتخزين البرامج والبيانات التي تقع تحت المعالجة، أي أن محتويات هذه الذاكرة قابلة للتعديل (حذف، إضافة، تغيير)، كما أنها تفقد محتوياتها بانقطاع التيار الكهربائي.

---

(20) أنظر زياد عبد الكريم وآخرون، الكمبيوتر وتطبيقاته، دار المستقبل للنشر والتوزيع، عمان، 1990م. ص21 وما بعدها.

(21) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص56.

(22) فراس محمد العزة وآخرون، مهارات الحاسوب الحاسوب والبرمجيات الجاهزة، المرجع السابق، ص14.

(23) علي حسن محمد طوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، جامعة عمان العربية للدراسات العليا، عمان، 2003، ص18.

ب. وحدة ذاكرة القراءة فقط: حيث تتم برمجة هذه الذاكرة (تخزينها بالبيانات المطلوبة) أثناء مرحلة التصنيع، ويمكن قراءتها عند الحاجة، ولا يمكن تخزين أي معلومات جديدة أثناء استخدامها، ولا تفقد هذه الذاكرة محتوياتها بانقطاع التيار الكهربائي.

3. وحدة الحساب والمنطق[24]: تقوم بإجراء العمليات الحسابية والمنطقية المطلوبة، وتتكون من مجموعة من الدوائر الحسابية والمنطقية ومجموعة من المسجلات اللازمة لتنفيذ العمليات المطلوبة.

4. وحدة التحكم: تنظم علاقة وحدة المعالجة المركزية مع الوحدات الاخرى لاستلام البيانات وارسال النتائج بعد المعالجة[25] فتقوم بالتحكم بعمل وحدات الحاسوب وتنسيق تبادل البيانات والأوامر وتحتوي على مجموعة من المسجلات والعدادات ودوائر فك الرموز وتحليلها ومولدات إشارات التزامن والتحكم.

5. وحدة الذاكرة المساعدة: وتستخدم لتخزين كميات هائلة من البيانات وبصورة دائمة، أي أنها لا تفقد محتوياتها بانقطاع التيار الكهربائي. ومن أهم وسائط التخزين المستخدمة الأقراص المرنة والأقراص الصلبة والأشرطة الممغنطة والأقراص المضغوطة، وتصل سعة القرص الصلب في الحواسيب الشخصية الحديثة إلى ما يزيد عن 40 غيغابايت[26].

6. وحدة الإخراج: وهي مجموعة الوحدات المسؤولة عن إظهار ما يحتاجه المستخدم للتفاعل مع الحاسوب وإيصال نتائج المعالجة للمستخدم[27]، باستقبال البيانات من

---

(24) محمد أحمد فكيرين، أساسيات الحاسب الآلي – دار الراتب الجامعية – بيروت – 1993م، ص51.

(25) فراس محمد العزة وآخرون، مهارات الحاسوب –الحاسوب والبرمجيات الجاهزة، المرجع السابق، ص14. أنظر محمد فهمي طلبة وآخرون، الموسوعة الشاملة لمصطلحات الحاسوب الإلكتروني، موسوعة دلتا كمبيوتر، مطابع المكتب المصري الحديث، القاهرة، 1991– ص34. وانظر د. علاء السالمي– تكنولوجيا المعلومات، ط1، كحلون–عمان، 1997، ص153.

(26) علي حسن محمد طوالبة، التفتيش الجنائي على بيئة الحاسوب والانترنت، المرجع السابق، ص19.

(27) فراس محمد العزة وأخرون، مهارات الحاسوب –الحاسوب والبرمجيات الجاهزة، المرجع السابق، ص14. وزياد القاضي وآخرون، المرجع السابق، ص 62.

الحاسوب وتمريرها إلى المستخدم بالصيغة المناسبة، أي إخراج نتائج المعالجة ومنها الشاشة والطابعة ومشغلات الأقراص.

ثانيا: البرمجيات software

وهي الكيان المنطقي للحاسوب وتتمثل في مجموعة التعليمات التي تهدف إلى إنجاز أعمال بواسطة نظام لمعالجة المعلومات يدعى الحاسوب...والبرامج بالإضافة إلى التوثيق الملحق به وأدواته التحضيرية[28].

ويعرف كذلك بأنه "مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات"[29]، إذن يشتمل الكيان المنطقي على جميع العناصر غير المادية اللازمة لتشغيل الكيان المادي فيشتمل على البرامج وصف البرامج والمستندات الملحقة بالبرنامج، وهو مصطلح أعم وأشمل من البرنامج، حيث يضم زيادة على البرنامج وصفه ومستنداته الملحقة.

وتنقسم الكيانات المنطقية إلى نوعين هما:

1. الكيانات الأساسية: وتضم كل البرامج الضرورية من أجل استخدام أفضل للحاسوب وملحقاته، وهي مندمجة في الجهاز ذاته مثل أنظمة التشغيل وأنظمة البرمجة[30].
2. الكيانات التطبيقية: وتضم هذه الفئة البرامج التي تمكن مستخدم الجهاز من أن ينفذ بواسطته عملاً محدداً بدقة ومتصلاً باحتياجات هذا المستخدم الخاصة والذي يسعى لمواجهة مشكلة ما. وتساعد المستخدم في عمله ومن أمثلتها برامج معالجة النصوص وجداول البيانات الإلكترونية وبرامج قواعد البيانات وبرامج التحليل الإحصائي وبرامج

---

(28) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص58.

(29) رشا مصطفى أبو الغيط- الحماية القانونية للكيانات المنطقية، برامج الحاسوب، وصف البرامج المستندات الملحقة، ملتقى الفكر، الإسكندرية، 2000م، ص5.

(30) محمد فهمي طلبة وآخرون، الموسوعة الشاملة لمصطلحات الحاسوب الإلكتروني، موسوعة دلتا كمبيوتر، مطابع المكتب المصري الحديث، القاهرة، 1991، ص 369.

لتطبيقات مختلفة مثل: الرسم والتصميم الهندسي والألعاب...الخ. ولا شك أن هذه الكيانات المنطقية تحتاج إلى الحماية القانونية نظراً لمساسها المباشر بحياة الأشخاص أو نشاط المؤسسات أو بعمل الهيئات. وما يتطلبه ذلك من حفاظ على سرية ما يتداول من معلومات وبعدها عن القرصنة والاعتداءات[31]. ومن هنا ظهرت الحاجة إلى تشريعات خاصة لحماية برامج ونظم الحاسوب وشبكة الإنترنت.

ثالثا: البيانات أو المعلوماتية data

التي تعد مطلب أساسي للتعامل مع الحاسوب ومن أجلها يتم إعداد البرامج فلكي يتم التوصل إلى المعلومات باستخدام الحاسوب يتم أولا البحث عن البيانات لتخزينها في الحاسوب ومعالجتها لتحويلها إلى معلومات[32]، وعرفتها الاتفاقية الاوروبية بأنها كل إبراز للحقائق والمعلومات أو المعاني في هيئة تقبل المعالجة في نظام الحاسوب بما في ذلك البرنامج الذي يجعل الحاسوب مؤهلا للعمل[33].

---

(31) محمد عبد الظاهر حسين، الاتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية، دار النهضة العربية، القاهرة، 2001/2000، ص17.

(32) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص61.

(33) الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي، المؤرخة 2001/11/23، المادة (1/أ).

المطلب الثالث

ماهية الانترنت

الانترنت هو جزء من ثورة الاتصالات ويعرف البعض الانترنت بشبكة الشبكات في حين يعرفها بعضهم بأنها شبكة طرق المواصلات السريعة. إن تمويل هذه الشبكة تحول من القطاع الحكومي إلى القطاع الخاص، مما ولد العديد من الشبكات الإقليمية ذات الصبغة التجارية والتي يمكن الاستفادة من خدماتها مقابل اشتراك، وتجدر الإشارة إلى أن عدم وجود مالك محدد أو معروف للإنترنت يجعل مهمة رجال الأمن أكثر صعوبة.

والانترنت(34) هو شبكة عالمية تربط عدة آلاف من الشبكات وملايين أجهزة الكمبيوتر المختلفة الأنواع والأحجام في العالم وتكمن فائدة الانترنت التي تسمى أيضا (the net) في كونها وسيلة يستخدمها الافراد والمؤسسات للتواصل وتبادل المعلومات.

بدأ العمل في الانترنت عام 1969 في وزارة الدفاع الامريكية إبان الحرب الباردة(35)، حيث كونت وزارة الدفاع الأمريكية فريق من العلماء لانجاز مشروع بحثي حول إنشاء شبكات تربط فيما بين أجهزة الحاسبات الالكترونية، لخدمة التأهب السريع للقوات المسلحة في حال نشوب حرب نووية أو أي هجوم عسكري عليها(36)، وبعد انهيار الاتحاد السوفييتي وانتفاء الهدف العسكري للشبكة تحولت إلى خدمة أغراض مدنية استفادت منها العديد من الشركات والجامعات والمؤسسات الخاصة.

وفيما يتعلق بتوسع الشبكة ففي عام 1985 كان هناك أقل من الفي حاسب آلي مرتبط بالشبكة وقد وصل هذا العدد إلى خمسة ملايين في عام 1995 وفي عام 1997 تجاوز العدد

---

(34) سلام فارس تتورين، دراسة تم تقديمها في الجامعة اللبنانية، الفرع الفرنسي، الدراسات العليا– قانون الاعمال المحلي والدولي.

(35) مقالة للعقيد محمد عبد الله منشاوي – باحث متخصص في دراسات جرائم الحاسوب والانترنت– مدير قسم الاحصاء والدراسات الجنائية.

(36) أحمد عبد الكريم سلامة، الانترنت والقانون الدولي الخاص– فراق أم تلاق، القانون والكمبيوتر والانترنت، المجلد الأول، 2004، ط3، ص25.

الستة مليون حاسوب، وتستخدم ما يزيد على ثلاثمائة ألف شبكة فرعية في أرجاء العالم، ويمكن القول إن عدد المستخدمين الجدد مليونان شهريا أي إنضمام ستة وأربعين مستخدماً جديداً للشبكة في كل دقيقة، وقدر عدد مستخدمي الشبكة عالميا حسب استطلاع شبكة (nua) الأمريكية عام 1998 بمئة وأربعة وثلاثين مليون مستخدم، وفي تقرير أجرته الشبكة ذاتها عام 2000 قدر عدد المستخدمين عام 2005 بمئتين وخمسة وأربعين مليون مستخدم[37]. يتم إدخال البيانات وسائر الخدمات الاخرى إلى الأجهزة كالمجموعات الاخبارية والاعلانات الترويجية والمزايدات والمناقصات والبريد الالكتروني عن طريق مقدمي خدمة الانترنت من الشركات المتخصصة في تكنولوجيا الاتصال[38].

إن إحداث المزج مابين الاتصالات والمعلومات من المسائل التي أدت إلى تحديث في نظرة الانسان إلى بيئة التقنية الافتراضية التي تجاوزت النظرة التقليدية الانسانية للزمان والمكان وحركة الاتصال مع سهولة استخدام تلك البيئة في الحالتين الايجابية منها والسلبية التي تصل معدلاتها إلى الحدود القصوى المتمثلة في الجريمة[39].

ويمكن النظر إلى الانترنت بوصفه مهداً للأمن الاجتماعي وخاصة في المجتمعات المغلقة والشرقية حيث أن تعرض هذه المجتمعات لقيم وسلوك المجتمعات الاخرى يسبب تلوث ثقافي يؤدي إلى تفسخ اجتماعي وانهيار في النظام الاجتماعي العام لهذه المجتمعات.

يوفر الانترنت العديد من الخدمات وأهمها[40]:

1. **البريد الإلكتروني:** لإرسال واستقبال الرسائل ونقل الملفات مع أي شخص له عنوان بريدي الكتروني بصورة سريعة جداً لا تتعدى ثواني.

---

(37) محمد عبدالله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، mohammed@minshawi.com، مكة المكرمة، 2003/11/1م.

(38) أحمد عبد الكريم سلامة، الانترنت والقانون الدولي الخاص، المرجع السابق، ص26.

(39) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراة، جامعة عين شمس- كلية الحقوق، 2004، ص223.

(40) محمد عبدالله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، mohammed@minshawi.com ، مكة المكرمة، 2003/11/1م.

2. **القوائم البريدية:** تشمل إنشاء وتحديث قوائم العناوين البريدية لمجموعات من الأشخاص لهم اهتمامات مشتركة.
3. **خدمة المجموعات الإخبارية:** تشبه خدمة القوائم البريدية باختلاف أن كل عضو يستطيع التحكم بنوع المقالات التي يريد استلامها.
4. **خدمة الاستعلام الشخصي:** الاستعلام عن العنوان البريدي لأي شخص أو جهة تستخدم الانترنت والمسجلين لديها.
5. **خدمة المحادثات الشخصية:** يمكن التحدث مع طرف آخر صوتا وصورة وكتابة.
6. **خدمة الدردشة الجماعية:** تشبه الخدمة السابقة وفي الغالب يمكن لأي شخص أن يدخل في المحادثة أو يستمع إليها دون اختيار الآخرين.
7. **خدمة تحويل أو نقل الملفات:** لنقل الملفات من حاسب إلى آخر خدمة نقل الملفات من حاسب إلى آخر.
8. **خدمة الأرشيف الإلكتروني:** تمكن البحث عن ملفات معينة قد تكون مفقودة في البرامج المستخدمة في حايب المستخدم.
9. **خدمة شبكة الاستعلامات الشاملة:** تفيد في خدمات كثيرة كنقل الملفات والمشاركة في القوائم البريدية حيث يفهرس المعلومات الموجودة على الشبكة.
10. **خدمة الاستعلامات واسعة النطاق:** تسمى باسم حاسباتها الخادمة وهي أكثر دقة وفاعلية من الأنظمة الأخرى حيث تبحث داخل الوثائق أو المستندات ذاتها عن الكلمات الدالة التي يحددها المستخدم ثم تقدم النتائج بشكل قائمة بالمواقع التي تحتوي المعلومات المطلوبة.
11. **خدمة الدخول عن بعد:** تسمح باستخدام برامج وتطبيقات في حاسب إلى آخر.
12. **الصفحة الإعلامية العالمية:** أو الويب، تجمع معا كافة الموارد المتعددة التي تحتوي عليها الانترنت للبحث عن كل ما في الشبكات المختلفة وإحضارها

بالنص والصوت والصورة، ويعد الويب نظام فرعي من الانترنت وهي النظام الأعظم كونه الشامل باستخدام الوسائط المتعددة.

ولكي يتمكن المستخدم من الاتصال بالانترنت يجب أن يتوافر لديه مجموعة من المستلزمات وهي حاسب آلي، جهاز مودم، خط هاتفي، الاشتراك في الخدمة، برامج تصفح الشبكة وأشهرها internet explorer[41]. وللاتصال بالانترنت لا بد من الاشتراك بخدمة الانترنت ويحصل هذا الاتصال عبر شبكة الهاتف أو الخط المخصص للاتصال بشبكة محلية زيادة على غيرها من الطرق الحديثة غير الشائعة إلا لاستخدامات معينة ومحصورة ببعض اجهزة الدولة[42].

([41]) محمد عبدالله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، mohammed@minshawi.com ، مكة المكرمة، 1\11\2003م.

([42]) سلام فارس تنورين، قانون الاعمال المحلي والدولي، المرجع السابق.

المبحث الثاني

ماهية جرائم الحاسوب

إن تحديد الأفعال المعتبرة أنماط للسلوك الإجرامي شهدت تطورا سريعا وتم تقسيم جرائم الحاسوب لعدد من الطوائف المختلفة مع ظهور انماط جرمية مستحدثة في الثمانينات، وقد ظهرت جريمة الاستخدام غير المصرح به لخدمات الحاسوب وجرائم غش الحاسوب وجرائم التلاعب بالمنافذ البنكية بواسطة البطاقات الممغنطة، وجرائم التوصل مع أنظمة الاتصال البعدي واختراق شبكات المعلومات واستخدام تقنية الفيروس في جرائم التلاعب بالبرامج والنظم وأنشطة قرصنة البرامج ونتيجة لذلك وضعت تشريعات لحماية حق التأليف. وسيتم التعرف على ماهية جرائم الحاسوب عبر مطلبين الأول سيتطرق لمفهوم هذه الجرائم وسيستعرض المطلب الثاني الطبيعة القانونية لها.

المطلب الأول

مفهوم جرائم الحاسوب

اشتقت كلمة الجريمة في اللغة من الجرم وهو التعدي أو الذنب وجمع الكلمة إجرام وجروم وهو الجريمة، إن تعريف الجريمة عموما "فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبير احترازي"، فهي كل فعل ضار يأتيه المواطن ويكون لهذا الفعل أثر ضار على غيره من المواطنين[43].

---

(43) سلام فارس تنوري، جرائم الحاسوب والانترنت، دراسة تم تقديمها في الجامعة اللبنانية – قسم الدراسات العليا، قانون الأعمال المحلي والدولي.

وحتى نصل إلى تعريف دقيق لوصف الجريمة عموما يجب أن يحوي التعريف عناصر هذه الجريمة المتمثل في السلوك، السلوك غير المشروع وفق القانون، الإرادة الجنائية وأثرها، التدبير الذي يفرزه القانون.

وتعرف جرائم الحاسوب والانترنت بأنها "سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الكمبيوتر"[44]، فالسلوك يشمل الفعل الإيجابي والامتناع عن الفعل، وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الجرمية، ومعاقب عليه قانونا لأن إصباغ الصفة الإجرامية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك حتى لو كان السلوك مخالفا للأخلاق.

ومحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة، بيانات ومعلومات معالجة ومخزنة، البرامج بأنواعها، المعلومات المستخرجة والمتبادلة بين النظم).

وأما الكمبيوتر فهو النظام التقني بمفهومه الشامل المزاوج بين تقنيات الحوسبة والاتصال بما في ذلك شبكات المعلومات، ومن دون نص القانون على النموذج القانوني للجريمة لا يتحقق إمكان المسائلة عنها سندا إلى القاعدة الشرعية الجنائية التي توجب عدم جواز العقاب عند انتفاء النص، وسندا إلى أن القياس محظور في ميدان النصوص التجريمية الموضوعية[45].

وتعرف جرائم الحاسب الآلي بأنها: "ذلك النوع من الجرائم التي تتطلب إلماما خاصا بتقنيات الحاسب الآلي ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعلها"[46]، كما يمكن تعريفها بأنها "الجريمة التي يتم إرتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي

---

(44) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الأزاريطة- الاسكندرية، 2005، ط2، ص179.

(45) تحت عنوان "جرائم الكمبيوتر والإنترنت المعنى والخصائص والصور واستراتيجية المواجهة القانونية"من خلال الموقع www.arablaw.org.com.

(46) ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص13.

بعمل غير قانوني"[47]، وهناك من عرفها بانها "أي عمل غير قانوني يستخدم فيه الحاسب كآداة أو موضوع للجريمة"[48]، وفي كل هذه الأحوال فجريمة الحاسب الآلي لا تعترف بالحدود بين الدول ولا حتى بين القارات فهي جريمة تقع في أغلب الأحيان عبر حدود دولية كثيرة[49].

لم يتفق الفقه على تعريف جامع مانع لجرائم الحاسوب فهناك العشرات من التعريفات يمكن ردها إلى مجموعات تبعاً للعناصر التي تضمنها التعريفات، وتوصلنا إلى أن تعريف الجريمة وفق معيار واحد، كتعريفها بالنظر لوسيلة ارتكابها فقط أو تعريفها حسب الضابط الشخصي (المعرفة الفنية لدى المجرم) وغيرها من المعايير إنما تظل عاجزة عن الإحاطة بمفهومها[50].

المطلب الثاني

الطبيعة القانونية لجرائم الحاسوب والانترنت

تختلف جريمة الانترنت عن الجريمة التقليدية التي تتسم بطابع خاص هو انها جرائم عابرة للحدود فهي تتم داخل الدولة ويكون تأثيرها منحصراً في تلك الدولة وإنما تلك الجرائم ترتكب عبر عدد من الدول لتتم في دولة أخرى وتكون آثارها ممتدة لتصل إلى عدد غير محدود من الدول. كما أن هذه الجريمة وفي جميع الاحوال يكون الحاسب الآلي هو آداة ارتكاب الجريمة وأن مرتكبها هو شخص ذو خبرة فائقة في مجال الحاسب الآلي ومحل هذه الجريمة هودائما المعطيات إما بذاتها أو بما تمثله[51].

([47]) جميل عبد الباقي الصغير، الانترنت والقانون الجنائي والأحكام الموضوعية للجرائم المتعلقة بالانترنت، ص23.

([48]) ذياب البداينة، الأمن وحرب المعلومات، ص102.

([49]) محمد عبدالله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، mohammed@minshawi.com، مكة المكرمة، 2003/1/1م.

([50]) نائل عبد الرحمن صالح، واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004،ط، 3من 1-3 مايو 2000م.

([51]) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص182.

تقوم جرائم الحاسوب وترتكز على المحاور التالية[52]:

1. أن الاعتداء على الكيانات المالية للحاسوب يخرج عن نطاق جرائم الحاسوب : لأن هذه الكيانات المادية محل صالح لتطبيق نصوص التجريم التقليدية الناظمة للجرائم الواقعة على الأموال.
2. أن محل جرائم الحاسوب هو دائما المعطيات "أما بذاتها أو بما تمثله، وقد تكون هذه المعطيات مخزنة داخل النظام أو على أحد وسائط التخزين أو تكون في طور النقل والتبادل ضمن وسائل الاتصال المدمجة مع نظام الحوسبة.
3. أن المصلحة محل الحماية في ميدان "جرائم الحاسوب" وهي الحق في المعلومات ككيان معنوي ذو قيمة اقتصادية عالية.

وعلية ظاهرة "جرائم الحاسوب" يمكن تعريفها وفق التحديد المتقدم بأنها:

"الأفعال غير المشروعة المرتبطة بنظم الحواسيب، أما تعريف جريمة الحاسوب فإنها "سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرميه لمعطيات الحاسوب"، فالسلوك شمل الفعل الايجابي والامتناع عن الفعل، وهذا السلوك ضمير مشروع باعتبار أن المشروعية تنفي عن الفعل الصفة ألجرميه، ومعاقب عليه قانونا لان أسباغ الصفة الإجرامية لا يتحقق في ميدان التشريع العقابي إلا بإرادة المشرع ومن خلال النص على ذلك، حتى ولو كان السلوك مخالفاً للأخلاق[53].

ومحل جريمة الحاسوب هو دائما المعطيات بدلالتها الواسعة (البيانات المدخلة والمخرجة والمخزنة والبرامج على أنواعها)، وأما الحاسوب فهو النظام التقني بمفهومة القائم على المزاوجة بين تقنيات الحوسبة والاتصالات أو ما يعرف "بالتقنية العالية".

([52]) نائل عبد الرحمن صالح، واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000م.

([53]) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000م.

ونظراً لحداثة عهد اللجوء إلى الحاسب الآلي خصوصا في الدول النامية ومنها الأردن وجدت المشاكل القانونية بوجه عام وتلك تدخل تحت طائلة قانون العقوبات بشكل خاص ذلك انه لا يوجد في الأردن تشريع يضع الحلول لتلك المشاكل فضلاً عن أنها لم تطرح على القضاء ليقول فيها كلمته، ومما يزيد الأمر تعقيدا أن الفقه القانوني الأردني لم يتناولها بالشرح والتحليل بشكل مسبق إذ أن الفقه يجري جاهداً وراء الاكتشافات العلمية الحديثة محاولا وضع الحلول القانونية اللازمة لما ينشا عنها من ظواهر إجرامية بعد أن تنشا وتستقر ويتكشف عن استخدامها الكثير من الظواهر الإجرامية الأمر الذي يضفي أهمية بالغة على هذا الموضوع[54].

إن التنوع في الجرائم الناشئة عن استخدام الانترنت يجعل التمييز قائما بين جرائم الحاسوب وبين جرائم الانترنت فليست كل جريمة ناشئة عن استخدام الانترنت تعد بالضرورة من جرائم الانترنت بل إن هناك من الجرائم ما يمكن وصفه بالجرائم التي كانت وسيلتها الانترنت ويقضي مثل هذا الامر تجريم الوسيلة في حين أنها بالطبيعة مشروعة[55].

وتعرف الوسيلة بأنها الطريقة التي يتم استخدامها من قبل مرتكب الجريمة لمباشرة السلوك المادي أو النشاط الاجرامي ولا تعد الوسيلة نشاطا ماديا وإنما يقرر القانون لزوم وجودها لكي يمكن إحداث تطابق بين النموذج الإجرامي وبين الواقعة ومن ثمّ استحقاق العقاب والإلزام بأن يعترف القانون بالوسيلة للقول بلزوم توافرها، وقرار المشرع بلزوم توافر وسيلة معينة يعني في القانون إضافة ظرف مشدد أو جعل العقوبة مشددة أو يجعل من اللازم اتخاذ تدابير معينة حيال مرتكب الجريمة[56].

([54]) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000م.

([55]) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراة، جامعة عين شمس- كلية الحقوق، 2004، ص224.

([56]) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراة، جامعة عين شمس- كلية الحقوق، 2004، ص249.

والانترنت لا يمكن أن يكون وسيلة إلى ارتكاب جرائم كونها بالأصل من الانشطة المشروعة ذلك أن الانترنت لا يمكن حيازتة واستخدامه بشكل ذاتي فهي ليست شيء ملموس وإنما سلوك تقني بالضرورة يحتاج لوسائل أخرى للقول بتوافرها. حيث تحتاج إلى الحاسوب ومكوناته على أن تكون مجموع الحواسيب متصلة فيما بينها مكونة شبكة ثم شبكات ثم ربط ذلك بحركة الاتصالات ونظم المعلومات يخلق بالنهاية بيئة معلوماتية كاملة حتى يمكن القول بتوافر الانترنت، فالانترنت ليست بيئة غير مشروعة أصلاً إنما يمكن ارتكاب أعمال إجرامية فيها أو من خلالها أو عبرها[57].

أركان جريمة الانترنت:

يتطلب المشرع للقول بقيام جريمة ما توافر الركن المادي والركن المعنوي لها، أما الركن المادي فيتكون من عناصره الثلاثة السلوك المادي والنتيجة الإجرامية والعلاقة السببية ما بينهما، أما الركن المعنوي بعنصريه العلم والإرادة[58].

الركن المادي في جرائم الانترنت

السلوك الاجرامي: إن ارتكاب الجريمة عبر الانترنت يحتاج إلى منطق تقني يتمثل بسلوك مادي إيجابي مما يجعل الجريمة عبر الانترنت ذات طابع موحد فهي تباشر من حيث السلوك أو النشاط المادي فيها بوصفه أحد عناصر الركن المادي يضاف إلى فلسفة الركن المادي فيها، تدارك هذا الأمر المشرع المقارن حين النص على جرائم يمكن أن ترتكب عبر الحاسوب ففي مثل هذه النصوص نجد المشرع يقرر صراحة عبارة "...إذا ارتكبت الجريمة باستخدام الحاسوب..." أو عبارة "... باستخدام المعالجة الآلية للبيانات..." ويكون بهذه الحالات المشرع

([57]) محمد أحمد فكيرين، المصدر السابق- ص 51 وما بعدها.. وانظر د. علاء السالمي- المرجع السابق- ص153.

([58]) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراة، جامعة عين شمس- كلية الحقوق، 2004، ص252.

مدركا للقيمة الموحدة للشروع في ارتكاب جريمة عبر الانترنت أو باستخدام الحاسوب المرتبط بالانترنت[59].

ضرورة استخدام الآلة وسيطاً لارتكابها مما يجعل جرائم الانترنت خاصة والحاسوب عامة من نوعية جرائم الوسيلة، وهذا الأمر غير مقبول لمشروعية هذا الوسيط المستخدم لارتكاب الجريمة وهو هنا الحاسوب أو الشبكة أو الخادم...وهذه أدوات مشروعة بحسب الأصل.

من اللازم استخدام الحاسوب لكي يمكن ارتكاب الجريمة التي ترتبط بإمكانية استخدام ومدى تمتع الشخص بالتقنية الكافية في هذا الشأن لارتكاب الجريمة، وأن كل من الحاسوب والانترنت يدخلان في طائلة المشروعية لا يمكن أن تقوم أي من الجرائم التي أشار إليها المشرع سوى باستخدامها وهذا يجعل مسألة استخدام الحاسوب والانترنت جزءاً من النشاط المادي في الجرائم الناشئة عن استخدام أي من الحاسوب والانترنت[60].

مما تقدم نرى أنّ النشاط المادي يبنى على العلاقة التقنية بين مرتكب جريمة الانترنت وبين الآلةوفي كيفية تحديد حدوث السلوك الإجرامي باستخدام الانترنت والحاسوب وجد المشرع الامريكي أن استخدام الانترنت ليس له هدف في ذاته فلا يستخدم الانترنت لمجرد الاستخدام وإنما هو تحقق فوائد عظيمة في الوقت الذي يمكن أن تكون مهدا لارتكاب الجريمة أيضا لذلك لم يمانع في تحديد طرائق السلوك الاجرامي بشكل تفصيلي لكي يمكن القول بقيام النشاط الاجرامي بما يجعل هذا النص ينطبق مع مراعاة تحقيق النتيجة المشار إليها[61].

العلاقة السببية مابين السلوك الإجرامي والنتيجة: وهي إسناد ماديات إلى مصدرها بشكل تسلسلي وهي من طبيعة مادية كأصل عام ، فالعلاقة السببية هي علاقة مادية وليست علاقة قانونية والمشرع يعترف بها قانونا صراحة أو ضمنا ولا يحيلها إلى الوصف القانوني بحيث تبرز

([59]) انظر :د. محمد فهمي طلبة وآخرون– المصدر السابق – ص122.

([60]) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراة، جامعة عين شمس– كلية الحقوق، 2004، ص257.

([61]) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراة، جامعة عين شمس– كلية الحقوق، 2004، ص 262.

كما لو كانت صلاحية في الانسان لإحداث أمرما فهي ليست مجرد علاقة أو رابطة زمنية لكونها عنصر رئيسي في الركن المادي للجريمة. والمبدأ العام الذي يحكم علاقة السببية أن الإنسان لا يسأل إلا عن النتائج التي يكون لنشاطه دخلا في إحداثها فاستحقاق العقاب في القانون الجنائي رهن دائماً بقيام الرابطة السببية بين نشاط الجاني وبين الواقعة الإجرامية التي تستوجب العقاب وذلك في معنى علاقة السبب بالنتيجة أو علة بالمعلوم لأنه مادام الجاني يعاقب على النتيجة التي أدى إليها فعله فإنه ينبغي لمسائلته أن تكون هناك رابطة بين ماديات الفعل وبين النتيجة الإجرامية[62].

ففي جريمة انتهاك الحق في الخصوصية عبر الانترنت يجب أن يكون هناك دخول على الانترنت باستخدام حاسوب عامل والقيام باختراق الخوادم المختلفة في مسارها ثم بعد ذلك التعدي على خصوصية موقع ما أو أن يقوم باعداد موقع ما ثم بعد ذلك يبث عليه في إحدى صفحاته صور ذات خصوصية لأشخاص مشهورين... الخ[63].

وتكون علاقة السببية قائمة بمجرد ثبوت الضرر في مجرد البث حيث؛ لأن علاقة السببية في الجريمة المتعلقة بحيازة صور دعارة الأطفال في حاسوب مضيف تتحقق بقيام رابطة بين العمل على إيجاد وحيازة هذه الصور في الحاسوب والانترنت وبين الترويج أو العرض أو التداول...الخ، والذي يحقق ضررا مباشر بالأطفال والقاصرين لكون ذلك يؤدي إلى انتهاك حقوق الاطفال المقررة. وكذلك القيام بإعداد الحاسوب وتهيئة الالتقاط مثل هذه الصور أو إعداد قرص صلب خاص بهذه الصور أو الأفلام وكذلك القيام بتخصيص برمجيات في القرص الصلب الخاص لكي يكون معد لعرضها. فكل هذه الأفعال يجب لكي تتم أن تقوم علاقة سببية بين

([62]) جميل عبد الباقي الصغير، الانترنت والقانون الجنائي والأحكام الموضوعية للجرائم المتعلقة بالانترنت، ص58.

([63]) انظر علاء السالمي- المرجع السابق- ص 153. زياد القاضي وآخرون، المرجع السابق، ص 62.

مباشرة النشاط المادي فيها وبين النتيجة المقررة هنا التي تبرز في ظهور النتيجة حال كونها كاملة أو الشروع في ارتكابها شرط الخيبة أو وقف ارتكابها بسبب لا دخل لارادة الجاني فيه[64].

النتيجة الإجرامية: وتعني النتيجة الاجرامية ذلك التغيير الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي والذي يعتد به القانون فيجعله عنصر من العناصر المكونة لجريمة معينة فلا تقع الجريمة تامة إلا بتوافره مع بقية العناصر الاخرى. فالنتيجة الإجرامية هي إحدى عناصر الركن المادي في الجريمة.

تثير النتيجة الاجرامية في جرائم الانترنت مشاكل متعددة حيث مسألة مكان وزمان تحقق النتيجة الإجرامية، فهل تعد هذه الجريمة مرتكبة سلوكا ونتيجة في العالم الافتراضي أو أن هناك امتداداً للنتيجة لكي يتحقق منتهاها في العالم المادي بينما يتحقق أولها في العالم الافتراضي ومن ثمّ يكون هناك امتداد في النتيجة من العالم الافتراضي إلى المادي؟ مع الأخذ في الاعتبار أن هناك من الجرائم التي يكون لها وجود سواء عبر الانترنت أم بمعنى أكثر وضوحا هي من ضمن جرائم التقنية التي لا يمتد أثرها إلى العالم المادي ويشمل ذلك بالطبع صعوبة اكتشافها وإقامة الدليل على ارتكابها ويتجه الفقه المقارن إلى محاولة إرساء رؤية الإفساد أو الإعاقة لكي تكون المحصلة في العمل الإجرامي ومن ثم فإن النهج هنا ينطلق نحو الاعتداء بالضرر في تقدير قيام المسئولية الجنائية حيث ينبغي وفقا لهذه النظرية الأخذ في الاعتبار ضرورة أن تكون كل علاقة وهمية على تعطيل الخدمات التي يقدمها الحاسوب للمستخدم الشرعي، كل ذلك يؤدي بالضرورة إلى الاهتمام بالنتيجة الاجرامية على حساب النشاط المادي للجريمة من حيث كونه الخلاصة النهائية التي ماتحرك المشرع المقارن إلا بسببها[65].

ويواجه تحديد الخطر أو الضرر بوصفه نتيجة إجرامية عبر الانترنت العديد من المشاكل كالمتعلقة بجرائم العدوان الفيروسي إذ تثير هذه النوعية من الجرائم مشكلة تحديد الضرر أو

([64]) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراة، جامعة عين شمس- كلية الحقوق، 2004، ص267.

([65]) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراة، جامعة عين شمس- كلية الحقوق، 2004، ص270.

الخطر وهي من الصعوبات التي تواجه الفكر القانوني المعاصر في هذا المجال خاصة إذا كان المشرع يتطلب تحقق نتيجة معينة، أما أثر النتيجة الإجرامية ذا البعد الدولي سواء في شكل امتداد الضرر أو الخطر إلى ما يتجاوز الحدود الاقليمية التي وقع فيها السلوك وبعض النتيجة ويأخذ هذا الامتداد شكل العدوان المحدد على مصلحة قائمة ومشروعة في دولة أو دول متعددة.

إن البحث في العلاقة بين النشاط وبين النتيجة الاجرامية يجعل منطق بناء النتيجة الاجرامية في جرائم الانترنت من الصعوبة بمكان، ذلك أنه كيف يمكننا القول أن النشاط الاجرامي المرتكب عبر الانترنت أدى بالضرورة إلى النتيجة المقررة في الجرائم التي يتطلب فيها المشرع حدوث نتيجة معينة فالمنطق هنا يسعى بنا إلى التأكيد على أن الجريمة عبر الانترنت ككل محل جدل إذ أن التغيير الحادث في العالم المادي والمؤدي إلى التقرير بوجود جريمة يظل جزاءاً منه إن لم يكن كله قد حدث في العالم الافتراضي ومن ثم يلزم الحال هنا التعرض لتأثير منطق العالم الافتراضي في العالم المادي لكي يمكن أن نتعرف على نوعية هذا التأثير الذي اعترف فيه المشرع المقارن[66].

إن كل جريمة تحدث باستخدام الانترنت إنما تحدث كلها أو بعضها حسب الاحوال في العالم الافتراضي وإذا كان النشاط المادي يحدث كله في العالم الافتراضي بما يستتبع ذلك علاقة السببية كذلك فإن النتيجة الاجرامية لها كان منفصلاً هنا حيث أنها تلك الجزئية التي تحدث بشكل انقسامي مابين حدوثها في العالم المادي جزئيا أم كليا، وذلك أمر استفهامي يقودنا حتماً إلى التقرير بالاهتمام بالنتيجة التي قررها المشرع تحديدا في نموذجه الاجرامي دون تمام التي تحدث تقنيا، فإذا تطلب المشرع القتل في جريمة إختراق قواعد بيانات المستشفيات مثلا بقصد ارتكاب جريمة قتل فإن تمام النتيجة تقنيا هو اكتمال تغيير بيانات الدواء ويلزم هنا لكي يمكن القول بتمام الجريمة على وفق تطلب النموذج القانوني للجريمة أن يتم إعطاء المريض الدواء الخاطئ فعلا فإذا لم يتم إعطاء المريض الدواء الخاطئ فإن الجريمة ماديا تضل في حالة شروع

([66]) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراة، جامعة عين شمس– كلية الحقوق، 2004، ص273.

شكلي ومن الناحية العملية فإن النتيجة الإجرامية التي يتم ارتكاب نشاط إجرامي ما عبر الانترنت بقصد الوصول إليها من الصعوبة بمكان إثبات القصد الإجرامي فيها توصلا إلى تحديد تسمية معينة للجريمة وذلك من الأمور التي تجعل الإثبات هنا قاصرا على التوصل إلى تحديدها بالدقة المتطلبة فقد يكتفي في مثل الجريمة السالفة بالاستعاضة عن جريمة الشروع بالقتل بجريمة تغيير أو تعديل بيانات اسمية أو العدوان على بيانات مرضية بما يشكل في النهاية عدوان على الحق في الخصوصية. سوف تظل مشكلة النتيجة الاجرامية في الجرائم الناشئة عن استخدام الانترنت محلا لجدل قانوني يجب أن يتم التطرق إليه من منطق التزاوج بين العالم المادي ونظيره الافتراضي بحيث يكون بناء معدلات الجريمة حين هيكلة ركنها المادي بالأخذ في الاعتبار هذا التزاوج.

الركن المعنوي في جرائم الانترنت: ويعني الجاني أو المجرم تحديدا فالركن المعنوي هو المسلك الذهني والنفسي للجاني باعتباره محور القانون الجنائي ذلك أنه في إطار هذا الركن تتوافر كافة مقومات المسئولية الجنائية من إسناد وإذناب مع إقرار حق الدولة في العقاب الذي يبنى على هذه المقومات، ويعرف الركن المعنوي بأنه العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني مرتكبها وهذه العلاقة هي محل الإذناب في معنى استحقاق العقاب ومن ثم يوجه إليها لوم القانون وعقابه. واجهت جرائم الحاسوب والانترنت مشكلات تتعلق بمدى تطلب القصد الجنائي فيها وبشكل يمكن أن يحقق غرض المشرع في هيكلة الادانه.

إن تفهم موقف الركن المعنوي في جرائم الانترنت يعد من الأمور الهامة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص العقابية التي يلزم تطبيقها إذ بدون الركن المعنوي لن يكون هناك سوى جريمة واحدة هي جريمة الدخول أو الولوج غير المشروع لذلك فإن اتجاه القضاء المقارن في تطلب العمد بالنسبة لجريمة الولوج فقط يعد من الموضوعات المنتقدة هنا، فالتمييز بين جريمة الدخول غير المشروع على نظام المعالجة الآلية للبيانات وبين جريمة تجاوز الصلاحيات في الدخول على مثل هذا النظام يعد تمييزاً دقيقا.

لم يستقر القضاء الامريكي على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام الانترنت من حيث تحديد ما إذا كانت تتطلب قصدا عام أم خاص فنجده لا يمانع في تطلب قصد جنائي خاص في جريمة التهديد إلا أنه يقرر من جديد أنه يستكفي بالقصد العام عن ذات الجريمة كما هو الشأن في جريمة التهديد بالبريد الالكتروني وعبر المجموعات الإخبارية. والقصد العام فيها يتم إستجلاء معالمه من النظرة الموضوعية إلى السلوك الشخصي من مجموعة الظروف المحيطة بالجريمة بما في ذلك فحص الحالة العقلية لمرتكب الجريمة[67].

أما القضاء الفرنسي فإن منطق سوء النية يكتسح النصوص الي تطبق بشأن الانترنت حتى أنه يخال أن هذه الجرائم لا يمكن أن تدخل حيز التطبيق مالم يتوافر سوء النية في منطق القصد الخاص وإرادة الإضرار حيث اشترط قانون العقوبات الفرنسي سوء النية حين وجود عدوان على البريد الالكتروني، كما ألزم تقنين البريد والاتصالات وزير الاتصالات الفرنسي بالسهر على مبدأ احترام سرة الاتصالات فالشرط الاساسي لتطبيق هذه النص مع الالتزام بضرورة توافر سوء النية هو وجود عدوان على الحق في خصوصية الاتصالات بما يستدعي ذلك أن يكون هناك وسيلة اتصال تتمتع بهذه الخصوصية أولا ومن ذلك البريد الالكتروني حيث يعد من وسائل الاتصال الخاصة والتي تتطلب بالضرورة حماية قوية.

---

(67) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراة، جامعة عين شمس– كلية الحقوق، 2004، ص294.

المبحث الثالث

ماهية جرائم الانترنت

من الصعوبة الفصل بين جرائم الحاسوب وجرائم الانترنت فلابد للأول لارتكاب الثاني[68]، تتسم جرائم الإنترنت والكمبيوتر بطابع خاص هو أنها جرائم عابرة للحدود فهي لا تتم من داخل دولة ويكون تأثيرها منحصراً في تلك الدولة وإنما تلك الجرائم ترتكب عبر عدد من الدول لتتم في دول أخرى وتكون آثارها ممتدة لتصل إلى عدد غير محدود من الدول وعليه فإن الأساس الذي يرتكز عليه مجال مكافحة الجرائم الإلكترونية هو التعاون الدولي وتنسيق الجهود المبذولة بين كافة دول العالم لتكون هناك نتائج مهمة يمكن الارتكاز عليها وتقويتها للحد من تلك الجرائم ذات النتائج البشعة على اقتصاديات الدول.

وعلى هذا الأساس فإن مكافحة الجرائم الإلكترونية لن يكون لها أي تأثير يذكر إلا إذا كان هناك تعاون دولي على أكبر قدر من التنسيق، للحصول على نتائج ملموسة تحد من ارتكاب تلك النوعية من الجرائم[69].

جرائم الإنترنت والكمبيوتر ذات خصائص متفردة خاصة بها لا تتوفر في أي من الجرائم التقليدية في أسلوبها وطريقة ارتكابها التي ترتكب يوميا في كافة دول العالم وتلك الخصائص الخاصة بجرائم الإنترنت هي:

(68) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com.

(69) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، "جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، 30 شارع سوتير الأزاريطة–الإسكندرية، 2005، ط2، ص179.

1 - في جميع الأحوال يكون الحاسب الآلي هو أداة ارتكاب الجريمة.

2 - ترتكب تلك الجرائم عبر شبكة الإنترنت.

3 - إن مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي.

4 - إن الجريمة لا حدود جغرافية لها.

محل جريمة الكمبيوتر هو دائما المعطيات إما بذاتها أو بما تمثله.

المطلب الأول

مفهوم جرائم الانترنت

تعد جريمة الانترنت من الجرائم المستحدثة التي تستخدم فيها شبكة الانترنت أداةً لارتكاب الجريمة أو لتسهيل ارتكابها، وأطلق مصطلح جرائم الانترنت في مؤتمر جرائم الانترنت المنعقد في استراليا عام 1998[70]. وتعرف جرائم الانترنت بأنها: جميع الأفعال الإجرامية المرتكبة بواسطة الحاسب الآلي من خلال شبكة الانترنت، ويشمل ذلك: الجرائم الجنسية والممارسات غير الأخلاقية، جرائم الاختراقات، الجرائم المالية، جرائم إنشاء أو ارتياد المواقع المعادية، جرائم القرصنة[71]. وهي مسألة ذات أبعاد خاصة سيما إذا أدركنا أن العالم الافتراضي هو نتاج اجتماع الاتصالات والتكنولوجيا والمعلومات التي تتجاوز منطق الحدود الدولية هو بيئة مناسبة لارتكاب أفعال يعدها المجرى العادي للامور في عالمنا المادي أفعال غير مشروعة تصل إلى التجريم في النظم الجنائية المعاصرة[72].

([70]) نائلة عادل محمد فريد قورة، جرائم الحاسبات الاقتصادية، دراسة نظرية وتطبيقية، ص26.

([71]) محمد عبدالله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، mohammed@minshawi.com، مكة المكرمة، 2003/11/1م.

([72])عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراة، جامعة عين شمس- كلية الحقوق، 2004، ص223.

وتعرف بأنها "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"[73] وكذلك تعرف بأنها "الجريمة الناتجة عن إدخال بيانات مزورة في الانظمة وإساءة استخدام المخرجات فضلاً عن أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر"[74].

وقد بينت إحصائيات الجمعية الأمريكية للأمن الصناعي أن الخسائر التي قد تسببها جرائم الحاسب الآلي للصناعات الأمريكية قد تصل إلى 63 بليون دولار أمريكي، وأن 25% من الشركات الأمريكية تتضرر من جرائم الحاسب الآلي وقد أصيب 63% من الشركات الأمريكية والكندية بفيروسات حاسوبية ووصل الفقد السنوي بسبب سوء استخدام الحاسب الآلي خمسمائة وخمس وخمسين مليون دولار[75].

ويصعب تحديد أن جرائم الحاسب الآلي المرتكبة هي الأكبر من حيث الخسائر حيث لا يعلن الكثير عن مثل هذه الجرائم ولكن من أكبر الجرائم المعلنة هي جريمة لوس انجلوس حيث تعرضت أكبر شركات التأمين على الاستثمارات المالية للإفلاس وبلغت خسائرها ملياري دولار أمريكي. وحادثة انهيار بنك بارينجر البريطاني في لندن إثر مضاربات فاشلة في بورصة الأوراق المالية في طوكيو حيث حاول البنك إخفاء الخسائر الضخمة بحسابات وهمية بمساعدة مختصين في الحاسب الآلي وقد بلغت إجمالي الخسائر حوالي ملياراً ونصف مليار دولار.

وكذلك نشر الفايروسات التي تضر بالأفراد والشركات وقد ينتج عنها توقف أعمالها نتيجة إتلاف قواعد بياناتها ويؤدي لخسائر مادية كبيرة –وصلت خسائر فيروس (code red) إلى ملياري دولار أمريكي، أما فايروس الحب الشهير وصلت خسائره 8.7 مليون دولار.

جرائم الانترنت كثيرة ومتنوعة ويصعب حصرها ولكنها بصفة عامة تشمل الجرائم الجنسية كإنشاء المواقع الجنسية وجرائم الدعارة أو الدعاية للشواذ أو تجارة الأطفال جنسيا وجرائم ترويج

---

(73) هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، ص20.

(74) واحد من عدة تعريفات وضعها مكتب المحاسبة العامة للولايات المتحدة الامريكية goa.

(75) محمد عبدالله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، المرجع السابق.

المخدرات أو زراعتها وتعليم الإجرام والإرهاب كصنع المتفجرات إضافة إلى جرائم الفيروسات واقتحام المواقع.

وإن كانت متابعة جرائم الحاسب الآلي والإنترنت والكشف عنها من الصعوبة بمكان حيث أن هذه الجرائم لا تترك أثرا فليست هناك أموال أو مجوهرات مفقودة وإنما هي أرقام تتغير في السجلات، ومعظمها تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها والتي لم تكتشف هي أكثر بكثير من تلك التي كشف الستر عنها[76].

ولا شك أن مستخدمي شبكة الانترنت في ارتكاب جرائمهم قد تجاوزوا الطرق التقليدية لما تتطلبه هذه الجرائم من ثقافة وخبرة تكنولوجية ومعلوماتية هائلة وهو أمر يقتضي التعرف على خصائص هؤلاء المجرمين وطبيعة جرائمهم.

خصائص المتهمين:

يتمتع نشطاء الانترنت بصفات وخصائص تميزهم عن غيرهم وذلك انعكاس حتمي لما تتطلبه عمليات استخدام هذه الشبكة من قدرات تقنية وفنية هائلة، بيد أن ذلك لا يعني حصر مرتكبي جرائم الانترنت في طبقة أو فئة معينة أو جنس معين، فمرتكب الجريمة قد يكون من البالغين أو الأحداث والمتعلمين منهم أو المثقفين ومن الفقراء والأغنياء ومن الرجال أو النساء، ولا يمكننا أن نحصر جرائم الانترنت في نوع معين من الجرائم فقد تكون من الجرائم الماسة بأمن الدولة من الداخل أو من الخارج وقد تكون من جرائم الاعتداء على الأشخاص أو جرائم الاعتداء على الأموال وقد تترتب على نشاط الجاني خسائر مادية غير محدودة تتجاوز الضرر المترتب على ارتكاب جريمة من الجرائم التقليدية.

وهؤلاء المجرمون يمكن تصنيفهم إلى الفئات التالية:

1- **القراصنة Les Pirates**

---

(76) محمد عبد الله منشاوي، جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com.

هناك صنفان من القراصنة[77]:

الصنف الأول: الهواة Hackers: وهم من الشباب الفضوليين الذين يسعون للتسلية ولا يشكلون خطورة على الصناعات وأنظمة المعلومات، فهم يتحدون إجراءات أمن النظم والشبكات، ولا تتوافر لديهم دوافع حاقدة أو تخريبية.

الصنف الثاني: المحترفون Crackers: وهم أكثر خطورة من الصنف الأول وقد يحدثون أضراراً كبيرة وقد يؤلفون أندية لتبادل المعلومات فيما بينهم، وتعكس اعتداءاتهم ميولا جرمية خطرة.

2- المخادعون Fraudeurs

وهؤلاء يتمتعون بقدرات فنية عالية باعتبارهم عادة من الأخصائيين في المعلوماتية ومن أصحاب الكفاءات، وتنصب معظم جرائمهم على شبكات تحويل الأموال ويمكنهم التلاعب بحسابات المصارف أو فواتير الكهرباء والهاتف أو تزوير بطاقات الاعتماد أو ما شابه.....الخ.

3- **الجواسيس Espions**

يهدف هؤلاء إلى جمع المعلومات لمصلحة دولهم أو لمصلحة بعض الأشخاص أو الشركات التي تتنافس فيما بينها[78].

([77]) تحت عنوان، جرائم الكمبيوتر والانترنت– المعنى والخصائص والصور واستراتيجية المواجهة القانونية، من خلال موقع: www.arablow.org.com.

([78]) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1–3 مايو 2000.

المطلب الثاني
وسطاء خدمة الانترنت

إن تشغيل شبكة الانترنت يتطلب مجموعة من الأشخاص قائمين على تشغيل هذه الشبكة وذلك لأن الانترنت عبارة عن أنشطة وأدوار عدة للعمل على تشغيل الأجهزة بتخزين المعلومات وبثها وعرضها، وهؤلاء الأشخاص هم الوسطاء في خدمة الانترنت[79]، فالوسطاء مجموعة من الأشخاص ينحصر دورهم في تمكين المستخدم من الدخول على شبكة الانترنت والتجول فيها والاطلاع على ما يريد فمنهم من ينقل الخدمة ومنهم من يمكن المستخدم من الوصول إلى الموقع ومنهم من يخزن المعلومات أو ينتجها أو يوردها.

أولا: مسئولية متعهدي الوصول

متعهد الوصول شخص طبيعي أو معنوي يقوم بدور فني بحت في أن يوصل العميل إلى شبكة الانترنت وذلك بمقتضى عقود اشتراك تضمن توصيل العميل إلى المواقع التي يريدها، واختلفت الآراء الفقهية في شأن تأصيل المسئولية الجنائية لمتعهدي الوصول حيث كانت في ثلاثة اتجاهات وهي[80]:

- **الاتجاه الأول:** يرى عدم مسئولية متعهد الوصول على الإطلاق لأن دوره فني بحت حتى ولو كان ضمن مهامه إيواء المعلومات إذ ليس بمقدوره وقف البث غير المشروع للمعلومات متى تضمن مادة معلوماتيه مخالفة للقانون، والمشكلة في حالة قيام متعهد الوصول باقتراح المادة المعلوماتية التي يتم بثها فهو بمثابة متعهد معلومات أو منتج ومن ثم يسأل جنائيا عن المادة غير المشروعة التي يبثها للجمهور عبر الشبكة.

([79]) جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، مرجع سابق، ص115.

([80]) عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، دار الفكر الجامعي، الازاريطة – الاسكندرية، ص134.

- **الاتجاه الثاني:** يرى مسئولية متعهد الوصول على أساس المسئولية التوجيهية فوضع المشرع نظام لكيفية النشر عبر الانترنت فهو ملزم بمحو ومنع الصور غير المشروعة ولا يعتد بدفاعه أنه لا يعلم فهو يعد موزع للمادة المعلوماتية ولكنه مجرد وسيط فني يقتصر دوره على توصيل المشترك بالإنترنت وبالتالي لا يمكن مسائلته.

- **الاتجاه الثالث:** يرى عدم مسئولية متعهد الوصول مطلقا ولكن يتوقف الأمر على طبيعة الدور الذي يقوم فيه، فهو يقوم بأدوار متعددة فقد يكون متعهد للإيواء أو التخزين أو ناقلا للمعلومات، ووفقا لهذا الرأي لو كان متعهد الوصول مجرد ناقل فلا تقام المسئولية الجنائية عن مراقبة المادة المعلوماتية التي يتم نقلها أما لو كان دوره غير ذلك فيسأل جنائيا.

أما خلاصة رأي القضاء كان كالآتي[81]:

لا يمكن إعمال قواعد المسئولية الجنائية المفترضة في حق موزع خدمة الانترنت لأن دوره فني بحت ينحصر في توصيل المشترك أو العميل بالمواقع التي يرغبها على شبكة الانترنت، فلا يحق له رقابة المادة المعلوماتية ومشروعيتها التي يقوم بنقلها، ونرجع للقواعد العامة للمسئولية الجنائية لإعمال مسئولية موزع خدمة الانترنت بأن يثبت أن له دوراً إيجابياً في بث مادة غير مشروعة مع وجود القصد الجنائي والقدرة الفنية على الرقابة.

ثانيا: مسئولية متعهد الإيواء[82]:

([81]) ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات العالمية، الجريمة عبر الانترنت، المرجع السابق، ص21.

([82]) القواعد العامة للمسئولية عبر شبكة الانترنت وشبكات الاتصالات الالكترونية، منشورات المنظمة المصرية لحقوق الانسان، 10/8 شارع متحق المنيل – منيل الروضة، القاهرة– مصر.

شخص طبيعي أو معنوي يعرض إيواء صفحات الـ web على حاسباته الخادمة مقابل أجر فهو بمثابة مؤجر لمكان على الشبكة للمستأجر (الناشر) الذي ينشر عليه ما يريد من نصوص أو صور أو ينظم مؤتمرات مناقشة أو ينشئ روابط معلوماتية مع المواقع الأخرى.

1. **المسئولية حسب القواعد العامة:** مؤلف المعلومات غير المشروعة وموردها عميل لدى متعهد الإيواء الذي يقوم بدوره بوظيفتي التخزين والإدارة للمعلومات حتى تصبح في متناول الجمهور فهو يتلقى الرسائل والأعمال من المؤلفين لنشرها على شبكة الانترنت بمقتضى عقد، فمورد المعلومات ينشىء الصفحات، أما متعهد الإيواء فهو يسهم في نشر هذه المعلومات عن طريق الوسائل الفنية التي يضعها تحت تصرف مورد المعلومات والذي هو في الأصل منشئ الصفحة على الانترنت.

ليس لتعهد الإيواء سيطرة على الصفحات التي يتولى تخزينها إلا إذا أصبحت بالفعل منشورة على الانترنت وقبل ذلك لا سيطرة له إلا إذا كانت الرسالة المحرمة مسجلة في وقت لاحق قبل إطلاع الجمهور عليها ويجب هنا أن نفرق ببين فرضين:

1. كون متعهد الإيواء شريكا في بث الرسالة غير المشروعة.
2. مسئولية متعهد الإيواء عن جريمة إخفاء أشياء مسروقة.

– **مسئولية متعهد الإيواء كشريك:** لا بد أن يثبت قيامه بفعل من أفعال الاشتراك وهي التحريض أو الاتفاق أو المساعدة، وهنا تكون المساعدة الإتيان بأفعال إيجابية تفيد مساهمته في السلوك الإجرامي للجريمة ويجب أن يقوم عليها دليل من الأوراق بعلم متعهد الإيواء بالطابع غير المشروع للمعلومات، ولا يسأل في حال ثبت عدم علمه بالمادة المعلوماتية غير المشروعة.

– **مسئولية متعهد الإيواء عن جريمة الإخفاء:** في حال وضعت المعلومات على ذاكرة الحاسب وهي غير مشروعة فلا تكون محلا للإخفاء كونها لا تمثل كياناً مادياً، أما إذا تم تسجيل تلك المعلومات غير المشروعة على قرص صلب مثلا فتقوم هنا جريمة الإخفاء.

2. **مسئولية متعهد الإيواء التوجيهية المفترضة:** أساس المسؤولية المفترضة أن تكون الرسالة غير المشروعة مسجلة قبل أن تصل إلى الجمهور والهدف حماية من يقومون بالبث

الإذاعي أو التلفزيوني المباشر إن وجدت مادة غير مشروعة لم يعلموا بها، والفقه الفرنسي يرى أن متعهد الإيواء لا علاقة له بالمسؤولية المفترضة بل هي تطبق على مدير النشر، ثم مؤلف الرسالة غير المشروعة، ثم المنتج، ومتعهد الإيواء لا ينطبق عليه دور من هذه الأدوار.

ثالثا: مسئولية المنتج:

إذا قام منتج الخدمة المعلوماتية في وسائل الاتصال السمعي والبصري بارتكاب جريمة بواسطة وسيلة للاتصال السمعي أو البصري فإن مؤلف الرسالة المعلوماتية متى تم تحريك الدعوة الجنائية ضده فإن منتج الخدمة يعاقب بوصفه فاعلاً أصلياً دون اشتراط سبق تسجيل المادة المعلوماتية حتى يقال بأنه مارس حقه في الرقابة كما هو الحال في مسئولية متعهد الإيواء.

رابعا: مسئولية ناقل المعلومات[83]:

ناقل المعلومات هو العامل الفني الذي يقوم بالربط بين الشبكات بمقتضى عقد نقل المعلومات من جهاز المستخدم إلى الحاسب الخادم لمتعهد الوصول ومنه إلى الحاسبات المرتبطة بمواقع الانترنت أو المستخدمين الآخرين من خلال الحاسبات المرحلة. فينحصر دورهم في نقل المعلومات وتأمين الربط بين الوحدات المختلفة ويفترض منهم عدم قيامهم بمراقبة الرسائل التي تمر من خلال شبكاتها، فلا يسأل هؤلاء عن المعلومات غير المشروعة، أما إذا كان يعلم بالطابع غير المشروع للمعلومات التي تعبر من خلال شبكته فإنه يسأل.

خامسا: مسئولية متعهد الخدمات:

([83]) القواعد العامة للمسئولية عبر شبكة الانترنت وشبكات الاتصالات الالكترونية، منشورات المنظمة المصرية لحقوق الانسان، 10/8 شارع متحق المنيل – منيل الروضة، القاهرة– مصر.

متعهد الخدمات هو ناشر الموقع وهو المسئول الأول عن المعلومات التي تعبر الشبكة وهو الوحيد صاحب السلطة الحقيقية لمراقبة المعلومات التي يجري بثها ويقع على عاتقه الالتزام بإخطار النائب العام بخدمة الاتصال السمعية والبصرية ويعين شخص طبيعي مديراً للنشر ليتحمل المسئولية الجنائية عن مضمون أو محتوى الخدمة.

سادسا: المسئولية الجنائية لمورد المعلومات:

مورد المعلومات هو الشخص الذي يقوم بتحميل الجهاز بالمعلومات التي قام بتأليفها أو جمعها حول موضوع معين، ومن ثم تكون له سيطرة كاملة على المادة المعلوماتية التي تبث عبر الشبكة ويمتلك جمعها من عدمه أو توريدها أو الامتناع عن ذلك ويسأل إذا ثبت قيامه بتسجيل أو بث معلومات غير مشروعة.

سابعا: مسئولية مؤلف الرسالة

مؤلف الرسالة هو المسؤول الأول عن أية معلومات غير مشروعة تتضمنها هذه الرسالة.

الفصل الثاني

جرائم الحاسوب

وتقسم جرائم الحاسوب والانترنت إلى مجوعة من الجرائم كالآتي:

المجموعة الأولى: تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي لاستغلالها بطريقة غير مشروعة كمن يدخل إلى إحدى الشبكات ويحصل على أرقام بطاقات ائتمان يحصل بواسطتها على مبالغ من حساب مالك البطاقة وما يميز هذا النوع من الجرائم أنه من الصعوبة بمكان اكتشافه ما لم يكن هناك تشابه في بعض أسماء أصحاب هذه البطاقات[84].

المجموعة الثانية: تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي بقصد التلاعب بها أو تدميرها كليا أو جزئيا ويمثل هذا النوع الفيروسات المرسلة عبر البريد الإلكتروني أو بواسطة برنامج مسجل في أحد الوسائط المتنوعة والخاصة بتسجيل برامج الحاسب الآلي وتكتشف هذه الفايروسات في معظم الحالات بواسطة برامج حماية مخصصة للبحث عن هذه الفايروسات ويشترط تحديث قاعدة بيانات برامج الحماية لضمان أقصى درجة من الحماية، مع أن وجود هذه البرامج في الحاسب الآلي لا يعني الحماية التامة من أي هجوم فيروسي

([84]) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com.

وإنما هو أحد سبل الوقاية التي بالإمكان اختراقها وإلحاق أذى بالجهاز ومكوناته خاصة إذا كان الفيروس حديث[85].

المجموعة الثالثة: تشمل استخدام الحاسب الآلي لارتكاب جريمة ما وقد وقعت جريمة من هذا النوع في إحدى الشركات الأمريكية التي تعمل سحبا على جوائز اليانصيب حيث قام أحد الموظفين بالشركة بتوجيه الحاسب الآلي لتحديد رقم معين كان قد اختاره هو فذهبت الجائزة إلى شخص بطريقة غير مشروعة[86].

المجموعة الرابعة: تشمل إساءة استخدام الحاسب الآلي أو استخدامه بشكل غير قانوني من قبل الأشخاص المرخص لهم باستخدامه كاستخدام الموظف لجهازه بعد انتهاء عمله في أمور لا تخص العمل[87].

([85]) يونس عرب، نظرية قانون الكمبيوتر، منشورات اتحاد المصارف العربية، 2001، من خلال الموقع: www.arablow.org.com.

([86]) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، المرجع السابق.

([87]) جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، مرجع سابق، ص128. انظر عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، المرجع السابق، ص151 وما بعدها.

المبحث الأول

الجرائم الواقعة على الحاسوب

سنقتصر في هذا المجال على التطرق إلى بعض أنواع الجرائم الأكثر انتشارا وشيوعاً ويضبط أغلب جرائم الحاسوب هذه معيار واحد وهو الاعتداء على الذمم المالية للغير "سواء أكان هذا الغير شخصا طبيعيا أو معنويا ، ويندرج تحت هذه الفئة صور ست نتناولها تباعا، ساعين في الوقت ذاته إلى محاولة إيجاد نصوص تشريعية جزائية تواجه كل منها :

1 - الجرائم الواقعة على الملكية الفكرية.

2 - جريمة سرقة منفعة الحاسوب.

3 - جرائم التزوير بواسطة الكمبيوتر.

4 - جرائم الاحتيال المعلوماتي.

5 - جرائم التخريب.

6 - جرائم التعرض لحرمة الحياة الشخصية.

المطلب الأول

الجرائم الواقعة على الملكية الفكرية

احد أهم الأسباب التي تعود إليها ظاهرة "قرصنة برامج الحاسوب"[88] هي ضعف وسائل الحماية القانونية للبرامج في معظم دول العالم الناتج عن الخلاف الفقهي التشريعي حول الطبيعة القانونية لبرامج الحاسوب، بسبب الطابع التقني الذي يميز هذه البرامج عن المؤلفات والمصنفات

---

(88) مصطلح القرصنة (Piracy) في اللغة هو: "السطو على سفن البحار" والقرصان هو لص البحر والقرصنة اصطلاحا هي السلب في أعالي البحر دون الحق أو سلطة مشروعة لم وقد استخدم تعبير القرصنة للدلالة على الفعال الاعتداء المستهجنة على المصنفات الأدبية والفنية، وأصبح لهذا المصطلح – منذ أمد بعيد دلالة واضحة على انتهاك حقوق التأليف والحقوق المخونة لمقتضى براءات الاختراع.

التقليدية، هذا فضلاً عن تباين مستوى الحماية لهذه البرامج من دولة إلى أخرى، مما يسبب لمنتجها مشكلات متعددة. ولقرصنة البرامج صورها وأشكالها المتعددة، تهدر أموال طائلة تقدر بالملايين في الدولة الواحدة المنصبة على أنشطة البحث والتطوير هذا عوضا عن هدر مبالغ طائلة تستخدم في مشاريع حماية برامج الحاسوب من مخاطر القرصنة تقنياً وإداريا بدلا من استخدامها في مشاريع الاستثمار والبحث وتطوير البرمجيات.

ويتطلب البحث في مسالة الحماية الجزائية لبرامج الحاسوب البحث في الطبيعة القانونية للبرامج الحاسوب بهدف تجديد القانون الذي يمكن من خلاله حمايتها وهذا ما ستتعرض له أولا على أن نتناول في البحث في جريمة تقليد برامج الحاسوب في قانون حق المؤلف الأردني رقم (12) لسنة 1992.

لم يبين قانون حق المؤلف الأردني المقصود ببرامج الحاسوب كمصنف محمى، وبالمقابل عرف قانون حق المؤلف في الولايات المتحدة الأمريكية برنامج الحاسوب بأنه مجموعة من التعليمات والأوامر التي يمكن استعمالها بشكل مباشر أو غير مباشر في الحاسب الالكتروني بغرض استخراج نتيجة معينة "، ويعرف جانب من الفقه برنامج الحاسوب بأنه تعليمات مكتوبة بلغة علمية معينة موجهة إلى جهاز تقني معقد الحاسب بغرض الوصول إلى نتيجة معينة.

وقد انقسم الفقه في مسالة تحديد الطبيعة القانونية لبرامج الحاسوب ، فمنهم من يرى أن هذه البرامج هي عبارة عن اختراعات تندرج حمايتها ضمن إطار الملكية الصناعية " كالقوانين الخاصة ببراءات الاختراع والعلامات التجارية" والاتجاه والآخر يرى في برامج الحاسوب أنها مصنفات فتحمى تبعاً لذلك بقانون حق المؤلف.

وبالنظر إلى الاتجاه الغالب في الفقه وفي قوانين حماية حق المؤلف ، وما أخذ به من قانون حق المؤلف الأردني ، وحيث أن الحماية الواردة في قوانين حق المؤلف تنصبِ أساسا على الإنتاج الفكري الأصيل مهما كانت صورته (مكتوبا أو مسجلاً، كلاماً أو أرقاما)، حيث أن شرط الأصالة (الابتكار)، يعتبر شرطاً أساسيا لشمول المصنف بحماية حق المؤلف، فإننا

نرى أن برامج الحاسوب لم تتمتع بصفة المصنفات وهي بذلك تخضع للحماية المقررة في قوانين حق المؤلف.

جريمة تقليد برامج الحاسوب في قانون حماية حق المؤلف الأردني (رقم 1992/2)

عرف الفقه جريمة تقليد المصنفات بوجه عام على أنها:

" كل اعتداء مباشر أو غير مباشر على حقوق التأليف في مصنفات واجبة الحماية "

وبتطبيق هذا التعريف على برامج الحاسوب يمكننا تعريف جريمة تقليد برامج الحاسوب بأنها " كل اعتداء مباشر أو غير مباشر على حقوق التأليف في برنامج الحاسوب".

وقد ورد النص على تجريم التقليد في المادة (51)[89] من قانون حماية حق المؤلف الأردني والتي يتضح من خلالها أن جريمة تقليد المصنفات – ومن بينها برامج الحاسوب – تستند إلى ركنين هما:

الركن الأول : الركن المادي بما يتطلبه من سلوك ونتيجة وعلاقة سببيه تربط بينهما ويتعلق النشاط الجرمي في جريمة تقليد برامج الحاسوب في قيام الفاعل بأحد أفعال التقليد المنصوص عليها في المادة (1/1/51) من ذات القانون المصنف محمي.

ومحل النشاط الجرمي في جريمة التقليد بصفة عامة هو المصنف المحمي وقد اعتبر قانون حق المؤلف الأردني برنامج الحاسوب من المصنفات المحمية بموجبة طبقا بما ورد في نص المادة (3/ب/8) من ذات القانون.

---

[89] نصت المادة (51) من قانون حق المؤلف الأردني على:

"أ. يعاقب بالحبس، مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن (500) دينار ولا تزيد على 1000 دينار، أو بإحدى هاتين العقوبتين:

* كل من باشر حق إحدى الامتيازات المنصوص عليهما في المواد (10،9،8) من هذا القانون.

* كل من يعرض للبيع مصنفاً مقلداً أو نسخاً عنه، مع علمه بأنه مقلد، أو يذيعه على الجمهور بأي طريقة كانت أو أدخلة إلى المملكة أو أخرجه منها

ب. وفي حالة التكرار لأي جريمة من الجرائم المنصوص عليها في الفقرة (أ) من هذه المادة يحكم على مرتكبيها بالحد الأعلى لعقوبة الحبس، وللمحكمة في هذه الحالة الحكم بإغلاق المؤسسة التي ارتكبت فيها الجريمة لمدة لا تزيد عن سن أو وقف ترخيصها لمدة معينة أو بصورة نهائية".

ولكي يتمتع برنامج الحاسوب بصفة " المصنف المحمي " فيكون محلا لجريمة التقليد فلا بد من توافر شرط الابتكار في البرنامج وفقاً لما ورد في حكم المادة (3/أ) من ذات القانون التي نصت على (أ. تتمتع بالحماية بموجب هذا القانون المصنفات المبتكرة في الآداب والفنون والعلوم أيا كان نوع هذه المصنفات أو أهميتها أو الغرض من إنتاجها).

ويتمثل السلوك أو النشاط الجرمي في جريمة تقليد برامج الحاسوب " في الاعتداء على حق من حقوق المؤلف التي نصت عليها المواد (8، 9، 10)[90] من القانون موضوع البحث ويجب لتحقيق هذا النشاط أن يقع الاعتداء فعلاً ولا يكفي هذا الاعتداء للقول بقيام النشاط الجرمي إذا لا بد من أن يكون الاعتداء قد وقع دون أذن من المؤلف. وبمعنى آخر فإن النشاط الجرمي في جريمة التقليد بوجه عام، ذو وجهان وجه ايجابي (الاعتداء)، والآخر سلبي (عدم موافقة المؤلف).

أما بالنسبة للإذن الكتابي الذي أشترط المشرع من المؤلف أو أحد خلفائه فإن تخلفه يعد أحد عناصر الركن المادي لجريمة التقليد، لأنه يعكس عدم رضى المؤلف عن الاعتداء الحاصل على مؤلفه. فالرضا في هذه الجريمة ليس محض ظرف موضوعي يعاصر أفعال الاعتداء التي يتكون منها الركن المادي للجريمة إنما هو احد عناصر الركن المادي فيها الذي يخلف بتخلفه، وعلى ذلك يعدّ عدم رضا المؤلف استغلال برنامجه عنصراً في الركن المادي لجريمة التقليد.

الركن الثاني: وهو الركن المعنوي: جريمة التقليد، جريمة مقصودة يستلزم قيامها توافر القصد الجرمي بعنصريه (العلم والإدارة): العلم بعناصر الجريمة وإرادة متجهة إلى السلوك الإجرامي ونتيجة ،هذا هو القصد الجرمي العام الذي يكفي لتوافر الركن المعنوي.

ولا تتطلب جريمة التقليد في ركنها المعنوي قصداً خاصاً إلى جانب القصد العام، فالمادة (1/أ/51) من قانون حماية حق المؤلف، لا يستنتج منها ضرورة توافر قصد خاص إلى جانب القصد العام، لدلالة ما يقرأ من المادة ذاتها:

([90]) تنص المادة (8) من قانون حماية حق المؤلف على ما يلي: " للمؤلف وحده".

" كل من باشر بغير حق ، أحد الامتيازات المنصوص عليها في المواد (8،9،10) من هذا القانون..." . وعليه فإنه يكتفي أن يعلم الجاني أن نشاطه الجرمي مرد على برنامج منسوب إلى غيره وأن تتجه إرادته إلى إذاعة أو نشر أو استعمال اقتباس هذا البرنامج حتى يتوافر بذلك القصد الجرمي.

وجدير بالذكر أن الفقه والقضاء الفرنسيين يتفقان على أن القصد الجرمي في جريمة التقليد مفترض ومؤدى ذلك أن تحقق إحدى صور النشاط الجرمي السابقة يعد قرينه كامنة للقول بتوافر القصد الجرمي وعليه فان حسن النية لا يفترض في نطاق جريمة التقليد مع الأخذ بعين الاعتبار أن هذه القرينة قرينه بسيطة تقبل أثبات العكس بحيث يقع على عاتق الجاني – إذا أراد نفي القصد – إثبات حسن نيته كي تبرأ ساحته عن الوقائع ألجرميه المنسوبة إليه والقول بتوافر حسن النية أو عدمه هو مسالة موضوعية تدخل ضمن صلاحيات محكمة الموضوع دون معقب عليها في ذلك من قبل محكمة التمييز، ما دام أن ذلك كان مبنياً على أسباب معقولة.

المطلب الثاني

سرقة منفعة الحاسوب

وتشمل الدخول غير المصرح به، وهو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاكات إجراءات الأمن، وكذلك الاعتراض غير المصرح به وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام كمبيوتر أو عدة نظم أو شبكة اتصالات[91]. ويقصد بسرقة المعلومات والبيانات المعالجة آليا الاستيلاء عليها دون علم وإرادة صاحبها الشرعي سواء أكانت مخزنة على أشرطة ممغنطة (ديسكات) أو أسطوانات مدمجة (سي دي)، فعلى سبيل المثال قد يوجه أحد الأشخاص البيانات الخاصة بالغير إلى حاسوبه

([91]) يونس عرب، موسوعة القانون وتقنية المعلومات، دليل امن المعلومات والخصوصية– جرائم الكمبيوتر والانترنت، منشورات اتحاد المصارف العربية، الجزء الأول، ط1، 2002، ص320.

الشخصي ويطلع عليها، أو يقوم بالتقاط الموجات الكهرومغناطيسية التي يبثها جهاز الحاسوب، ثم يعالجها ويظهرها من جديد بشكل واضح على شاشة تلفزيون[92].

يقوم عنصر المال المنقول في السرقة على ثلاثة مقومات يتعين اجتماعها معاً فيجب أن يكون موضوع السرقة مالا، ويجب أن يكون هذا المال ذا طبيعة منقولة، ويتعين أخيراً أن يكون مملوكا للغير.

أولاً : لزوم أن يكون موضوع السرقة مالاً: تصنف السرقة على أنها من جرائم الاعتداء على الأموال وذلك لآن فعلها المادي وهو الاختلاس لا يقع إلا على مال[93]. بل أن علة تجريم السرقة هي أنها اعتداء على ملكية هذا المال والملكية هي أحد الحقوق العينية، وقد نصت المادة 81 من القانون المدني المصري على أن "كل شي خارج عن التعامل بطبيعة أو بحكم القانون يصلح أن يكون محلاً للحقوق المالية"[94]. ويخرج الشيء عن التعامل بطبيعته إذا كان من الأشياء التي لا يستطيع أحد أن يستأثر بحيازتها، كما يخرج الشيء عن التعامل بحكم القانون إن حظر القانون أن يكون هذا الشيء محلا للحقوق العينية، ولكي يعتبر الشيء مالا يجب أن تكون له قيمة، فالمال هو كل شيء يمكن تقويمه ومع ذلك لا تشترط في المال المسروق قيمة معينة[95]. لكن قيمة الشيء لا يشترط أن تكون مادية، بل يصح أن تكون قيمة معنوية (مع كون الشيء نفسه له قوام مادي).

ويتفق ذلك مع وصف الجانب المادي من مكونات النظام الآلي لمعالجة المعلومات كما قد يبدو أنها لا تتعارض مع وصف الجانب غير المادي من مكونات النظام الآلي بأنه مال. ولكن

([92]) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000.

([93]) محمود مصطفى، شرح قانون العقوبات، القسم الخاص – القاهرة 1984 – دار النهضة الغربية – ط8، ص464.

([94]) حسن صادق المرصفاوي، قانون العقوبات الخاص – الإسكندرية – جلال حرى – سنة 1991، ص 286.

([95]) نقض :1913/5/1 المجموعة الرسمية ص 14 مشار إليه لدى المرصفاوي في قانون العقوبات تطوراته التشريعية ومذكراته الإيضاحية والأحكام في مائة عام للأستاذ الدكتور حسن صادق المرصفاوي، طبعة 1985 – رقم 3384، ص 1081.

العقبة في طبيعة هذا المال ذلك أن هذه المكونات لا تخرج عن دائرة التعامل لا بطبيعتها ولا بحكم القانون فهي قابلة لآن تكون محلا للحقوق المالية... وأن كانت محلا بالفعل للحقوق الذهنية[96] من هنا يصعب القول بوقوع هذه المقومات غير المادية للنظام الآلي لمعالجة المعلومات، محلاً لجريمة السرقة.

إن هذه المقومات غير المادية تتكون في حقيقتها من البرامج والبيانات أو المعلومات إضافة إلى جهد الآلة التي تقوم بإجراء المعالجة الآلية فالبرنامج هو إبداع (ابتكار) فكري وذهني قابل للاستغلال المالي. وحقيقة البرنامج ودورة ووظيفته هي انه أسلوب عمل، أي أسلوب لمعالجة المعلومات, ومن ثم فإن استخدام البرنامج دون وجه حق أي دون أذن أو أتفاق مع واضعه أو منتجه هو في الحقيقة اعتداء على حقوق الاستغلال المالي لهذا "المصنف". وهذا ما قد يسمى في بعض الحالات سرقة أدبية أو قد يسمى " تقليداً " للمصنف فإذا وقع الاعتداء على البرنامج فهو اعتداء على حقوق المؤلف في استغلال مصنفة استغلالا مالياً. ومن ثم يرد علية أحكام حماية حق المؤلف.

أما المعلومة فهي تسجيل لواقع قائم كحالة أو رقم أو صفة...الخ، قد تكون سرية بمعنى أن يكون الاطلاع عليها أو حيازتها محظوراً وفي هذه الحالة فإن الحصول عليها الواقع ممن لا صفه له في ذلك يمثل انتهاكاً لسرية المعلومة وليس سرقة لها. أما إذا كانت المعلومة غير سرية، أي أن العلم بها مباح للكافة، فلن يخرج الأمر هنا عن أحد فرضين الأول أن تكون المعلومة مجانية، وهنا لا جريمة في الحصول عليها. وأما الثانية أن تكون المعلومة متاحة للكافة بمقابل مادي، وهنا فأن الحصول عليها بغير المقابل المحدد لها ، وبغير رضاء من له الحق في تقاضي هذا المقابل يكون في حقيقته سرقة للمنفعة أو الفائدة المرجوة من هذه المعلومة، والمرجع في تجريم ذلك إلى أن وجود نص أو عدمه[97].

([96]) محمود نجيب حسني، شرح قانون العقبات القسم الخاص – القاهرة 1986، رقم 1901 وما بعدها، ص810 وما بعدها.

([97]) عمر الفاروق الحسيني، لمحه عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، القانون والكمبيوتر والانترنت، المجلد الأول، ط3، 2004، ص333.

أخيراً فأن جهد الآلة ما هو إلا خدمة تتاح مقابل مادي أيضا، ومن ثم فالحصول على هذه الخدمة بغير المقابل المقرر، وبغير لقاء صاحب الحق في اقتضاء ذلك المقابل، وهو أيضاً سرقة للمنفعة بالمعنى المتقدم.

ثانيا: كون المال منقولاً: والمال المنقول في نطاق القانون الجنائي أوسع مدلولا منه في نطاق القانون المدني ، فقد نصت المادة 1/82 من القانون المدني على أن كل شيء مستقر بحيزه ثابت فيه لا يمكن نقلة منه دون تلف فهو عقار وكل ما عدا ذلك فهو منقول, ولكن في القانون الجنائي فأن كل مال يمكن نقلة من مكان إلى آخر يعد منقولا حتى إن كان نقله يعرضه للتلف، فانتزاع حجر غير مملوك للجاني بنية تملكه يعد سرقة، واقتلاع شجرة من الأرض أو قطعها بنية تملكها يعد سرقة أيضاً [98].

فالمال المنقول ينبغي أن يكون كيانه مادياً لا معنوياً[99] فالحق الفكر مفاهيم معينة لا ترد عليها سرقة وإنما تجوز السرقة للسند المثبت لهذا الحق كالسند المثبت للدين، أو إيصال الأمانة وللمخطوط الذي سجل فيه المؤلف أفكاره[100] ووفقا للمستقر في الفقه أن " كل الأشياء المادية القابلة للانتقال من يد إلى يد تكون محلاً للسرقة سواء كانت من الأجسام الصلبة أو السائلة أو الغازية[101].

نجد أن عناصر النظام الآلي لمعالجة المعلومات في ضوء ما تقدم بالنسبة للبرنامج والمعلومة، فليس لأي منها قوام مادي مستقل بذاته، ومع ذلك من الممكن تحيزه في دعامة ما، كاسطوانة مثلاً أو شريط أو صورة ... الخ، ومن ثم هذه الدعامة هي التي تكون قابلة للسرقة بغض النظر عن قيمتها. بينما يبقى البرنامج أو المعلومة خارج دائرة السرقة لعدم تحقق وصف

([98]) رؤف عبيد، جرائم الاعتداء على الأشخاص والأموال، الطبعة الثامنة، السنة 1985، ص330.

([99]) إظهاراً لأهمية الطبيعة المادية في المنقول، فأنه قد يخصص أليها أحيانا موضع في الدراسة تدرس فيه كعنصر قائم بذاته إلى جانب المال ووصفة كمنقول – راجع مثلاً أ.د محمود نجيب حسنى، المرجع السابق رقم 1092.

([100]) محمود نجيب حسنى، شرح قانون العقوبات، القسم الخاص، القاهرة، 1986، ص812.

([101]) محمود محمود مصطفى، شرح قانون العقوبات، المرجع السابق، ص 466.

المال فيه لذاته وان أمكن تحيز كل منهما في إطار مادي، ويظل الاعتداء على أي منهما خاضعاً للأوصاف التي أوضحناها فيما تقدم[102] بالنسبة لجهد الآلة أو ساعات عملها فأن هذا الجهد لا يمكن أن نختزله إلى مجرد القوى المحركة للآلة من كهرباء أو غيرها، لنقول من ثم أن سرقة قد حدثت بالاستيلاء أو باختلاس جهد الآلة، وإنما واقع الأمر أن هذا الجهد هو محصلة لعدة أمور .ومن هذه الأمور القوى الكهربائية المحركة للآلة، هذا صحيح، ولكن هذه القوى ليست هنا هي المقصودة أساسا بالسرقة، أو بالاستخدام غير المشرع، وإنما المقصود بذلك هو "تكنيك" هذه الآلة أي التقنية التي يتمتع بها، وهذه التقنية لا يمكن تحيزها كالقوى الكهربائية مثلاً، وإنما هي تستخدم أو يتم الحصول عليها من مجرد تشغيل الآلة، وتنتهي بإيقافها، ولا يمكن اختزانها لفترة لاحقة على ذلك. ولهذا فإن جهد الآلة لا يمكن تحيزه مادياً فضلاً عنه انتفاء صفة المال بذاته عنه كما رأينا سلفاً ومن ثم فانه لا يصلح في باب السرقة إلا أن يكون محلا لسرقة المنفعة فقط.

ثالثاً : أن يكون المال المنقول مملوكاً لغير الجاني: الواقع أن الشرط قد يبدو أنه لا يثير صعوبة خاصة، بالنسبة "للأموال" المتعلقة بالمعلومات المعالجة أليا، تختلف عن الصعوبة التي يثيرها عادة في ملكية الصور التقليدية من الأموال المنقولة متى وقعت عليها سرقة. والسبب في ذلك استعمال لفظ الأموال هنا، فكيف يكون ثمة مال ولا يكون قابلاً للتمليك؟

لذلك نقول أن انتفاء صفة المال بذاته عن عناصر نظام المعالجة الآلية للمعلومات يستتبع بداهة أن الحق الوارد عليه ليس حق ملكية ومن ثم فإن كان ثمة عنصر أو ركن جوهري لحدوث السرقة أن يكون هناك اعتداء على الملكية فإن جريمة السرقة مستحيلة لانتفاء ذلك العنصر. فالرابطة الموجودة بين عناصر الجانب غير المادي من هذه النظم وبين صاحبها هي حق ذهني.

([102]) فوزية عبد الستار، شرح قانون العقوبات القسم الخاص – القاهرة – 1983، رقم 782، ص 702 وما بعدها.

وبالنسبة للبرنامج ولجهد الآلة فلا تتصور صعوبة في مثل هذا القول[103]، وكذلك الأمر بالنسبة للمعلومة التي هي تسجيل لواقع كما قلنا، وذلك بمراعاة ما جرى عليها من تصنيف وتبويب ومعالجة أنشأت لمن قام بذلك حقاً ذهنياً عليها ولا يستثنى من ذلك إلا المعلومة السرية التي لا يجوز قانوناً التعامل المالي فيها، أي التي تخرج عن دائرة التعامل بنص القانون أو بطبيعتها.

أما محل جريمة السرقة في قانون العقوبات الأردني محل هذه الجريمة "بالمال المنقول المملوك للغير"، والمدلول القانوني للمال – وفق أحكام المواد (53–54) من القانون المدني الأردني "هو كل عين أو حق له قيمة مادية في التعامل" و "كل شيء يمكن حيازته مادياً أو معنويا والانتفاع به انتفاعا مشروعا ولا يخرج عن التعامل بطبيعة أو بحكم القانون يصح أن يكون محلا للحقوق المالية" هكذا ونلاحظ انه يشترط حتى ينطبق وصف المال على الشيء (وهو هنا المعلومة والبيانات المعالجة آليا) أن يتوافر فيها شرطان هما:

أ– القابلية للحيازة ب– الانتفاع المادي بها.

وتوصف المعلومات والبيانات بالأموال المعنوية إلا انه في الوقت ذاته لا يمكن اعتبارها منقولات، وذلك للأسباب التالية[104]:

أ. يتطلب القانون في المال المنقول أن يكون من طبيعة مالية مرئية محسوسة والمعلومات ليست كذلك.

ب. أن نص هذه المعلومات والبيانات (بالمعنى المجازي للنقل) لا يؤدي إلى إشغال الحيز الذي كانت – هذه المعلومات قبل نقلها.

([103]) أحمد فتحى سرور الوسيط في قانون العقوبات القسم الخاص – القاهرة – الطبعة الثالثة سنة 1992، ص786.

([104]) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1–3 مايو 2000م.

اشترط قانون العقوبات الأردني كما هو سائر التشريعات العربية في المال محل جريمة السرقة أن يكون من الأموال المنقولة، فإن البيانات والمعلومات المعالجة آليا لا تصلح وبالنظر لطبيعتها غير المادية، وعدم قابليتها للنقل أن تكون محلا لجريمة السرقة.

فلا يمكن اعتبار النشاط الجرمي مؤلفاً لجرم السرقة، وقد يتبادر إلى الذهن فيما إذا كان من الممكن اعتباره مؤلفاً لجريمة(105) اعتراض الرسائل المنقولة عبر شبكات الاتصال "خلافاً لأحكام المادة (76) من قانون الاتصالات الأردني رقم (13) لسنة 1995و/أو جريمة اعتراض موجات مخصصة للغير خلافاً لأحكام المادة (80) من ذات القانون ؟.

إن سلوك الشخص الذي يعترض البيانات المنقولة عبر شبكات الحواسب فيوجهها إلى حاسوبه وبعد عرضها، يعتبر سلوكا مجرما وفقا لحكم المادة (76) من القانون المذكور، وفي الوقت ذاته فإن هذا السلوك يعتبر مجرما أيضا وفق حكم المادة (80) من ذات القانون، ذلك أن اعتراض موجات شبكات الحواسيب (والمملوكة فنياً وقانونياً للشركة مالكة الشبكة المخترقة) مجرم صراحة وفقا لحكم المادة (80) سواء أكان هدف الجاني من هذا الاعتراض توجيه الموجات الحاسوبية وإعادة ترجمتها أم لا. وبطبيعة الحال، فإن المحكمة في هذه الحالة تطبق على الجاني العقوبة الأشد عملا بأحكام التعدد المعنوي للجرائم (م57 من قانون العقوبات الأردني)(106).

إلا أن هذا الحكم يقتصر على الاستيلاء على المعلومات والبيانات وينصر على حالة انتقال المعلومات من وحدة طرفية إلى أخرى (أي من حاسوب لآخر)، ولا تشمل صورا أخرى

---

(105) المادة 76 من قانون الاتصالات كل من اعتراض، أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصال، أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد عن ستة أشهر أو بغرامة لا تزيد على (300) دينار أو بكلتا العقوبتين ". ومن ذات القانون نصت المادة (80) محلى ين كل من قام معتمدا باعتراض موجات مخصصة للغير أو بالتشويش عليها باستخدام موجات كهرومغناطيسية بدون ترخيص يعاقب بالحبس مدة لا تزيد عن ستة أشهر أو بغرامة لا تقل عن (50) دينار ولا تزيد عن (200) أو بكلتا العقوبتين".

(106) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1−3 مايو 2000م.

للاستيلاء أو السرقة. وعليه فإننا نتمنى على المشرع الجزائي الأردني التدخل لتجريم كافة صور السرقة والاستيلاء على المعلومات والبيانات المعالجة آلياً في أجهزة الحاسوب .

المطلب الثالث

تزوير مكونات الحاسوب

ويشمل تزوير الكمبيوتر أو التزوير المعلوماتي بإدخال أو إتلاف أو محو أو تحوير المعطيات أو البرامج أو أية أفعال تؤثر على المجرى الطبيعي لمعالجة البيانات ترتكب باستخدام الكمبيوتر وتعد فيما لو ارتكبت بغير هذه الطرق من أفعال التزوير المنصوص عليها في القانون الوطني[107].

دفع تزايد التلاعب في الحواسيب لا سيما تلك العائدة للبنوك والمؤسسات المالية، فقهاء القانون الجزائي إلى محاولة اعتبار من يتلاعب بالبيانات آليا مرتكبة لجريمة التزوير في المحررات وكتبت مؤلفات وأبحاث حول موضوع تزوير معطيات الحاسوب، وانقسم الرأي في الفقه حوله بين مؤيد ومعارض، إلى أن حسمت المسالة في التشريعات الغربية بتدخل المشرع بنصوص صريحة تجرم سائر أشكال تزوير معطيات الحاسوب في الحالات التي ينجم عنها ضرر للغير[108].

وللوقوف على مدى كفاية النصوص الناظمة لجريمة (التزوير في المحررات)[109]. في قانون العقوبات الأردني في مواجهة هذه الصور المستحدثة من جرائم الحاسوب، نستعرض فيما يلي أركان هذه الجريمة وهي :

([107]) يونس عرب، موسوعة القانون وتقنية المعلومات، دليل امن المعلومات والخصوصية- جرائم الكمبيوتر والانترنت، منشورات اتحاد المصارف العربية، الجزء الأول، ط1، 2002، ص320.

([108]) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000م.

([109]) نصت المادة (260) من قانون العقوبات الأردني على أن "التزوير، هو تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد أثباتها بصك أو مخطوط يحتج بهما نجم أو يمكن أن ينجم عنها ضرر مادي أو معنوي أو اجتماعي.

1 – الركن المادي والمتمثل في تغيير الحقيقة في محرر.

2 – الركن المعنوي والذي يمثل القصد الخاص.

3 – ركن الضرر والذي لا يشترط المشرع وقوعه فعلاً إنما يكتفي باحتمال وقوعه.

وهدياً بمقتضيات أحكام تلك المادة وأركانها فإننا لا نتردد في القول بان أحكام هذه الجريمة لا يمكن أن تنطبق على أفعال تطوير معطيات الحاسوب وذلك للأسباب التالية :–

1. حكم شروط جريمة التزوير أن يقع تغيير الحقيقة في محرر، وهذه الصفة لا تنطبق على معطيات الحاسوب، ذلك أن قراءة البيانات المعالجة أليا (بغض النظر عن مكان تخزينها) حكر على الجهاز فقط.

2. لو سلمنا جدلا بان صفة (المحرر) تنطبق على معطيات الحاسوب، فإن عقبة أخرى تقف دون تطبيق نصوص جريمة التزوير في المحررات عليها، إذ يشترط لتوافر هذه الجريمة أن يكون لهذه المحررات حجية في الإثبات بالمعنى المقصود في قانون البيانات وهو ما لا يتوافر في معطيات الحاسوب ولا مستخرجاته؟ فإذا كان قانون البيانات الأردني لا يسمح بقبول معطيات الحاسوب كبينة في الدعاوي الحقوقية – ولا يضفي عليها قوة ثبوتيه، فكيف نعطيها هذه الصفة ونحن بصدد البحث في جريمة، محلها دائماً المحرر المكتوب لقبول الاحتجاج به قانونا.

يعزز هذه الاستنتاج ما ذهبت إليه محكمة التمييز الأردنية في القرار رقم 82/30 حيث قضت "أن استعمال الصورة الفوتوستاتية المزورة غير المصدقة من أي مرجع رسمي لا يستلزم العقاب، لأن قانون البيانات لا يعطى ملك هذه الصورة أي قيمة في الإثبات".

حيث انه إذا جرى استعمال الكمبيوتر لإجراء عملية تزوير في مستندات بعدما جرى مسحها ضوئيا بواسطة السكانر (Scanner) وتم التلاعب بمحتوياتها بواسطة برامج الكمبيوتر ثم جرى استخدامها ورقياً بواسطة الطابعة فالتزوير يقع تحت الأحكام العامة للتزوير التي نصت عليها قوانين العقوبات. وقد يقع التزوير على مستندات مخزنه في ذاكرة الكمبيوتر يتم عرضها

على شاشته دون طباعتها ورقياً مما يستبعد تطبيق الأحكام العامة التي ترعى التزوير طالما أنها تفترض وجود مستند ورقي مكتوب أو مطبوع[110].

أما في التشريع الفرنسي فنرى أنه يمكن تطبيق نص المادة 462 فقرتها الرابعة المعدلة بموجب قانون 1988/1/5 التي تنص على أن كل من يتعرض بإرادته أو بمعرض عدم احترامه لحقوق أصحاب العلاقة بشكل مباشر أو غير مباشر فيدخل بعض المعلومات في النظام الآلي لمعالجة المعلومات أو يمحو أو يعدل فيها أو في طريقة المعالجة أو النقل لهذه المعلومات يعاقب بالسجن من ثلاثة أشهر إلى ثلاث سنوات وبالغرامة من ألفين إلى خمسمائة ألف فرنك فرنسي أو بإحدى هاتين العقوبتين، هذا هو الحال في فرنسا أما في الدول العربية فيبقى من الضروري إيجاد نصوص ترعى هذه المسائل لئلا يبقى المجرم دون عقاب[111].

المطلب الرابع
جرائم الاحتيال المعلوماتي

تعددت تعريفات جريمة الاحتيال المعلوماتي وتعددت تسمياتها فاستخدام بعض الفقهاء تسمية الغش المعلوماتي واستخدام آخرين تسمية غش الحاسوب هذه التعريفات تلتقي جميعها حول وصف الجرم بأنه سلوك احتيالي أو خداعي مرتبط باستخدام الكمبيوتر بهدف مرتكبه إلى تحقيق فائدة أو مصلحة ماليه. وقد نشأت هذه الجريمة مع شيوع أنظمة نقل وتحويل الأموال بالطريقة الالكترونية Electronic Fund Transfer حيث تزايد بشكل ملحوظ قيمة الأموال

([110]) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000.

([111]) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000م.

المتداولة بهذه الطريقة مما جعلها تصبح موضوعا لجرائم التحويل الإلكتروني غير المشروع للأموال[112].

فالاحتيال أو الغش المرتبط بالكمبيوتر فهو القيام بأية أعمال تؤثر بمجرى المعالجة الآلية للبيانات وتؤدي إلى إلحاق الخسارة أو فقدان الحيازة أو ضياع ملكية شخص وذلك بقصد جني الفاعل منافع اقتصادية له أو للغير[113]، ويعرف غش الحاسوب أو الاحتيال المعلوماتي بأنه (كل سلوك احتيالي يرتبط بعملية التحسيب الالكتروني بهدف كسب فائدة أو مصلحة مالية)[114]. فأيا كان شكل التلاعب في نظام الحاسوب فإن غش الحاسوب ينصرف الاعتداء على المعطيات المخزنة في النظام، بما يمثله من أموال وأصول وخدمات بهدف الحصول على منفعة مادية، ويرى العاملون بأمن الحاسوب أن أساليب ارتكاب (الاحتيال المعلوماتي) لا تخرج عن أربع وسائل هي:

1 - التدخل والتلاعب في مدخلات النظام.

2 - زرع برامج الفيروسات.

3 - التلاعب في معطيات الحاسوب عن بعد.

4 - التلاعب في البرامج.

وهذه الجرائم يمكن ارتكابها من موظفي البنوك ممن يملكون التقنية والكفاءة العالية للتلاعب بالبيانات عن طريق إدخال معلومات مصطنعة ، كذلك المبرمجين الذين يكلفون بتحديث وصيانة البرامج المصرفية مما يمكنهم من التلاعب بهذه البرامج هؤلاء يتمكنون أحيانا من اختلاس بعض الأموال من الأرصدة الموجودة في المصارف بتحويلها من حساب إلى آخر،

---

(112) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000م.

(113) يونس عرب، موسوعة القانون وتقنية المعلومات، دليل امن المعلومات والخصوصية- جرائم الكمبيوتر والانترنت، منشورات اتحاد المصارف العربية، الجزء الأول، ط1، 2002، ص320.

(114) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000.

وإذا ما تمكن احدهم من التزود بكلمة السر، أو بمفتاح الشيفرة وأداة الربط، قد يتمكن بنتيجة ذلك من التلاعب بأرقام الحسابات. والأمثلة على هذا النوع من الجرائم كثيرة تحفل بها النشرات المتخصصة بهذه المواضع ونذكر منها الآتي: الجريمة التي تمكنت شرطة مرسيليا من القبض على مرتكبيها وهو مستخدم يعمل في إحدى المصارف، تمكن بواسطة استعمال كمبيوتر الفرع حيث يعمل، من إجراء تحويلات أموال وهمية إلى حساب خاص باسمه في سويسرا[115].

وقامت موظفة في إحدى المصارف في جنوب ألمانيا في عام 1983، وكانت أمينة صندوق في هذا المصرف، تمكنت من خلال التلاعب في البيانات من تحويل مبلغ (1.3) مليون مارك ألماني إلى حساب صديقها. ولكن جريمتها هذه تم اكتشافها في اليوم نفسه الذي جرى فيه عملية التحويل بفضل تطور أنظمة الرقابة على الرغم من أن صديقها تمكن من سحب جزء كبير من هذا المبلغ بواسطة تنظيم شيكات. وقد حصلت جرائم مماثلة في بنك Zurich في سويسرا بعدما تمكن المجرم، وهو مستخدم في البنك المذكور، من تعطيل البرامج التي وضعت للتحويل دون التلاعب بالبيانات، وتمكن من إدخال بعض المبالغ المحولة من الخارج إلى حسابه الخاص[116].

الجرائم التي تحصل في المصارف على وفق التقنية المعروفة بـ Salami التي تقوم على الاستيلاء على الأموال بكميات صغيرة جداً من الحسابات الكبيرة بحيث لا يلاحظ نقصان هذه الأموال التي تحول من عدة حسابات إلى حساب خاص يستطيع الجاني سحب الأموال منه بشكل عادي. والسؤال الذي يطرح في هذا المجال هو كيف يمكن تطبيق أحكام قوانين العقوبات على هذا النوع من الجرائم، ليس فقط من زاوية القاعدة القانونية لأن الأمر لا يطرح أية مشكلة

([115]) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1–3 مايو 2000م.

([116]) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1–3 مايو 2000م.

كما أن القضية هي اعتداء على الأموال، وإنما من زاوية اكتشاف الجرم واثبات حصوله وتقدير قيمة الضرر اللاحق بالضحية[117].

أما وصف الجرم نفسه فهو من جهة إجراء تغيير وتلاعب في البيانات لإيهام صاحب الحساب بصحتها مما يجعله يسلم بها. ومن جهة ثانية إجراء تزوير في البنود المتعلقة بالحسابات وهو من جهة ثالثة استيلاء على أموال الغير دون رضاه ومن جهة رابعة إساءة أمانة إذا ما حصل من الشخص المكلف بحكم وظيفته بالمحافظة على هذه الأموال. ويبقى أن نقول في هذا المجال بأن الوصف القانوني لهذه الجرائم يختلف باختلاف الفاعلين وكذلك باختلاف الظروف التي أدت إلى ارتكابها.

فما مدى إمكانية اعتبارها مؤلفة لجريمة معاقب عليها في ضوء أحكام قانون العقوبات الأردني، وفي حقيقة الأمر فإنه ليس في هذا القانون نص خاص يحسم بصورة قاطعة جريمة "غش الحاسوب" إلا انه وبالمقابل فقد نظم قانون "جريمة الغش" بوجه عام في الفصل الثاني من الباب الحادي عشر في المواد من (714-421) تحت عنوان "الاحتيال وسائر ضروب الغش"، أما تعبير الغش فيظهر واضحاً في الفصل الرابع من ذات القانون في المواد (428-437)، وباستعراض أحكام المادة (417) الناظمة لجريمة الاحتيال ، فإننا نجد أن هذه الجريمة لا تقع في قانون العقوبات إلا: إذا توصل الجاني وبإحدى الطرق المحددة حصراً إلى الاستيلاء على المال بخداع المجني عليه وعملية الخداع هذه (وهي محور جريمة الاحتيال) تتطلب من المجني علية عقلا يفكر فيما يعرض عليه من أمور فيفوت الجاني عليه – بعد أعمال فكره – وجه الحقيقة أو الصواب ويقع في الغلط ويتصرف في المال تبعاً لذلك[118].

([117]) جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، مرجع سابق، ص132. عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، دار الفكر الجامعي، الازاريطة – الاسكندرية، ص134. أنظر وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، المرجع السابق.

([118]) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000م.

وعليه، فإننا نرى أن من يمارس وسائل احتيالية في مواجهة نظام معالجة آلية للبيانات فيتمكن من اختراقه بهدف تحقيق منفعة مادية أو الحصول على خدمة لا يكون مسؤولاً عن جريمة الاحتيال بمفهومها السابق وندلل على صحة هذا الاستنتاج، بأن نظام معالجة المعلومات "الحاسوب" أو "العقل الالكتروني" يفتقر إلى خاصية التفكير (قوام عملية الخداع)، فالعقل الإلكتروني لا يفكر بالمعنى الدقيق لهذه الكلمة، بقدر ما ينفذ أوامر تلقاها أو تلقى أسلوب معالجتها مسبقاً. فضلاً عن ما تقدم أن معطيات الحاسوب (محل جريمة الاحتيال) ذات طبيعة معنوية، وهي بذلك تفتقر إلى شرط المشرع في محل جريمة الاحتيال بكونه مالا منقولا ذا طبيعة مادية.

المطلب الخامس

إتلاف مكونات الحاسوب

التخريب هو كل عمل من شانه أن يلحق ضرراً بشيء ما فيؤدي إلى إفساده وانعدام جدواه، ويشمل الإضرار بالبيانات والبرامج بمحو أو تعطيل أو تخريب معطيات الكمبيوتر وبرامجه، وتشمل كذلك الإدخال أو المحو أو الإتلاف أو التخريب أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر أو نظام الاتصالات (الشبكات)[119].

وهو في موضوعنا الحاضر قد يقع على أحد الأمور التالية:

أولاً: الأجهزة Hardware وهي أشياء مادية كجهاز الكمبيوتر نفسه أو الطابعة Printer أو الماسحة الضوئية Scanner أو الغير ذلك من الأجهزة ، أن تخريب هذه الأجهزة لا يثير أي مشكلة من زاوية العقوبة طالما أن قوانين العقوبات تشمل أحكاما ترعى هذا النوع من الجرائم

([119]) يونس عرب، موسوعة القانون وتقنية المعلومات، دليل امن المعلومات والخصوصية– جرائم الكمبيوتر والانترنت، منشورات اتحاد المصارف العربية، الجزء الأول، ط1، 2002، ص320.

باعتبارها من جرائم الاعتداء على الأموال فيمكن تطبيق هذه القواعد وبالتالي فإن الموضوع لهذه الجهة لا يتمتع بأية خصوصية[120].

إذا كان المقصود بتخريب البرنامج هو تخريب القرص الضوئي أو الاسطوانة التي استعملت لتخزين البرنامج، فيمكن العودة إلى أحكام التعدي على الأموال باعتبار أن هذه الاسطوانات هي أموال مادية، أما إذا كان المقصود هو الاعتداء على البرنامج نفسه باعتباره مجموعة من المعطيات واللوغاريتمات فإن الوضع يختلف حتماً ويرتدي من ثم طابعاً على شيء يسير من الدقة ومن المعلوم إن تخريب البرامج من الجرائم الشائعة جداً والصحف والمجلات المتخصصة تذخر بالكثير عن القصص حيث يتم فيها تصوير المجرمين كأبطال يتمتعون بمستويات عالية من الذكاء والنباهة مما يمكنهم من تحدي كبريات الشركات والمؤسسات[121].

قضية المحاسب المتخصص في المعلوماتية الذي دفعته رغبة الانتقام، بعد صرفه من عملة في إحدى الشركات، إلى التلاعب ببرامج المحاسبة في الشركة مستخدماً مهارته مما أدى إلى محو المعلومات بتاريخ حدده هو، فبعد ستة أشهر من عملية الصرف فوجئ مدير الشركة بذلك وعن كيفية معاقبة عمليات التخريب أتجه رأي في الفقه القانوني الغربي إمكانية تطبيق أحكام قانون العقوبات التي ترعى قضايا التعدي على الأموال. لكن هذا الرأي سرعان ما سقط لا سيما بعدما تم الأخذ بعين الاعتبار السببين الآتيين:

1. إن الأحكام العامة تتحدث عن التعدي على الأملاك أو الأموال المادية ولا يمكنها أن تشمل المعلومات والبرامج باعتبارها ملكية فكرية ومعنوية لا يمكن التباس في موضوعها على الأموال المادية.

([120]) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000م.

([121]) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000م.

2. إن التخريب قد يشمل، ليس فقط إفساد البرامج أو المعلومات بل قد يقتصر على إجراء بعض التعديلات فيها وهذا ما قد يخرجه عن إطار التخريب المادي الذي يفترض تعرضاً مادياً يلحق ضرراً قد لا يلحقه التعديل في البرامج.

وبنتيجة هذا الجدال حسم الأمر في فرنسا على وجوب وضع قوانين خاصة جرى دمجها بإحكام قانون العقوبات اعتباراً من مطلع العام 1988، هذه الأحكام الخاصة تسري على تخريب البرامج وكذلك أيضاً على تخريب المعلومات، ويمكن تلخيصها بما يأتي حيث المادة 462-2 المعدلة بموجب قانون 1988/1/5 التي تعاقب بالسجن ما بين شهرين وعامين أو بالغرامة ما بين عشرة آلاف ومائه ألف فرنك فرنسي، كل ما تعرض بشكل غير مشروع للنظام التشغيلي فأدى إلى إفساده أو تعطيله بسبب محو أو تعديل للمعلومات الموجودة فيه.

وكذلك المادة 462-3 التي تشدد العقوبة المنوه بها أنفا بجعلها السجن من ثلاثة أشهر إلى ثلاث سنوات والغرامة من عشرة آلاف أو مائه ألف أو إحدى هاتين العقوبتين إذا ما جرى ارتكاب الجرم المذكور آنفاً بفعل إرادي.

أما المادة 462-4 تتناول بشكل خاص موضوع التعرض للمعلومات فتنص على أن كل من يتعرض بإرادته أو بمعرض عدم احترامه لحقوق أصحاب العلاقة، بشكل مباشر أم غير مباشر ،فيدخل بعض المعلومات في النظام الآلي لمعالجة المعلومات أو يمحو أو يعدل فيها أو في طريقة المعالجة أو النقل لهذه المعلومات يعاقب بالسجن من ثلاثة أشهر إلى ثلاثة سنوات وبالغرامة من ألفين إلى خمسمائة ألف فرنك فرنسي أو بإحدى هاتين العقوبتين.

المطلب السادس

جرائم التعرض لحرمة الحياة الشخصية

مع تطور وسائل الاتصال، واستخدام أجهزة الكمبيوتر في هذا المجال، أصبحت المعلومات تتداول على الشبكات بشكل متزايد بحيث أصبح من الممكن إجراء عمليات تقاطع المعلومات بسرعة وفعالية، لا شك بأن لهذا التطور فوائده وحسناته ولكن مساوئه لا سيما إذا ما

تعلق الأمر بمعلومات شخصية تمس حياة الأفراد الخاصة، وقد بدأ الوعي لخطورة الكمبيوتر على حرمة الحياة الخاصة في الدول الغربية منذ ما يزيد عن الثلاثين سنة، فتعالت صيحات حماة الحياة الخاصة لمواجهة أخطار المعالجة الآلية للبيانات الاسمية Tratement automatise de donnes nominate لا سيما في فرنسا حيث صدر بتاريخ 6 كانون الثاني 1978 قانون بهذا الخصوص بهدف إلى حماية الحياة الخاصة من مخاطر المعلوماتية فنص على عدد من الجرائم التي يعاقب عليها إذا لم تراع بعض القواعد في أثناء جمع المعلومات وفي مرحلتي المعالجة والتخزين في ذاكرة الكمبيوتر [122].

ومن هذه الجرائم جريمة معالجة البيانات الاسمية دون الحصول على ترخيص بذلك من المرجع المختص وهو اللجنة الوطنية للمعلوماتية والحريات NIL، وكانت أولى الأحكام الصادرة في هذا المجال عن القضاء الفرنسي الحكم الصادر عن محكمة nantes (نانتس) في 16/كانون الأول /1985 حيث عوقب الفاعل بالسجن لمدة شهرين وبدفع غرامة مقدراها عشرون ألف فرنك فرنسي. علماً بأن القانون المذكور نص على عقوبة الحبس في مثل هذه الحالة من ستة أشهر إلى ثلاث سنوات وبالغرامة من ألفي فرنك فرنسي إلى مائتي ألف فرنك فرنسي أو بإحدى العقوبتين (المادة الحادية والأربعون)[123].

ومن هذه الجرائم أيضا تلك التي تنطوي على الانحراف عن الغرض أو الغاية من المعالجة الآلية للبيانات الاسمية كما حددت في طلب الترخيص المقدم إلى اللجنة الوطنية للمعلوماتية والحريات المنوه بها أنفا. هذا الانحراف يؤدي في بعض الحالات إلى إساءة استخدام هذه المعلومات ويقع تحت طائلة المادة الرابعة والأربعين من القانون المذكور التي تعاقب بالسجن من سنة إلى خمس سنوات وبالغرامة من عشرين ألف إلى مائتي ألف فرنك فرنسي أو بإحدى هاتين العقوبتين ويشترط بطبيعة الحال للقول بهذه الجريمة توافر الركن المعنوي، فضلاً

([122]) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000م.

([123]) حست طاهر داوود، جرائم نظم المعلومات، المرجع السابق، ص239 ومابعدها.

عن الركن المادي، عندما تتجه إرادة الفاعل إلى فعل الانحراف عن الغاية المعالجة لهذه المعلومات.

ومن هذه الجرائم ما نصت عليه المادة الثالثة والأربعون من القانون الفرنسي المتعلقة بتخزين معلومات شخصية يشكل إفشاؤها تعرضاً للشرف أو الاعتبار أو حرمة الحياة الخاصة دون موافقة صاحب العلاقة. ويعاقب مرتكب هذا الجرم بالسجن من شهرين إلى ستة أشهر وبالغرامة من ألفين إلى عشرين ألف فرنك فرنسي أو بإحدى هاتين العقوبتين ومنها أيضا جرائم التسجيل والحفظ غير المشروع للبيانات الاسمية لفترة أطول من المدة المقررة في الترخيص الصادر عن اللجنة الوطنية للمعلوماتية والحريات CNFL لما في ذلك من خطورة على ما يسمى بحق النسيان في ما يتعلق بالجرائم التي يرتكبها بعض الأفراد بعدما تنقضي فترات معينه على ارتكاب هذه الجرائم . ويعاقب من يقوم بالتسجيل والحفظ لهذه المعلومات بالغرامة من مائتي إلى ألفي فرنك فرنسي وبالسجن من ستة أشهر إلى سنة واحدة أو بإحدى هاتين العقوبتين على ما نصت عليه المادتان /28/و/42/ من القانون الفرنسي المذكور آنفاً[124].

هذه الفئة من جرائم الحاسوب التي ترتكز على الاعتداء على الحرية الشخصية للأفراد من خلال ما يسمى "ببنوك المعلومات"، حيث تتضمن هذه البنوك بيانات تتصل بنواح خاصة وأحوال شخصية، تتعلق بحياة الأفراد، والتي يحرصون على أحاطتها بنوع من السرية والكتمان ولا يريدون لأي كان أن يطلع عليها[125]. وقد ارتبط هذا النشاط الإجرامي المستحدث بشيوع استخدام الحاسوب الذي نشأ ونما في الدول المتقدمة تكنولوجيا، وعانت شعوبها من مضاره وآثاره إلى أن تدخل المشرع الجزائي وخف عن حدة الاعتداء على الحرية الشخصية من خلال سن التشريعات الجزائية الرادعة.

وتضم هذه الفئة من فئات جرائم الحاسوب صورا متعددة نذكر منها :

([124]) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000م.

([125]) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000م.

1 - جمع وتخزين البيانات الشخصية بصورة غير مشروعة.

2 - إفشاء البيانات الشخصية.

3 - المعالجة الآلية للبيانات الشخصية دون ترخيص .

4 - تجاوز الغرض أو الغاية من المعالجة الآلية للبيانات الشخصية.

5 - استخدام بيانات شخصية معالجة آلية، بشكل غير صحيح.

إن هذه الأنماط السلوكية الجرمية، وأن تعددت صورها ، فإن موضوعها (محلها) هو واحد دائماً، وهو ما يعرف بالبيانات الاسمية والتي تعرف على أنها (البيانات الشخصية التي تتعلق بالحق في الحياة الخاصة للمرء كبيانات الخاصة بحالته الصحية والمالية والوظيفية والمهنية والعائلية عندما تكون هذه البيانات محلاً للمعالجة الآلية.

فما مدى إمكانية إسناد "جريمة إفشاء الأسرار" التي نظمت أحكامها المادة 355/2 من قانون العقوبات بحق من يأتي سلوكاً من شأنه أي يؤدي إلى الاعتداء على المعطيات ذات الطبيعة الخاصة المخزنة في بنوك المعلومات، بالأخذ بعين الاعتبار أن محل أو موضوع جريمة إفشاء الأسرار هي المعلومات ذات الطبيعة السرية، أما إفشاء البيانات الاسمية فمحلها البيانات الشخصية المعالجة آلياً بنظام الحاسوب، ومن جهة أخرى فإن الأسرار في جريمة الشخصية المعالجة آليا بنظام الحاسوب ومن جهة أخرى فإن (الأسرار في جريمة إفشاء الأسرار يشترط أن تكون: إما رسمية أو متعلقة ببعض المهن التي تفترض عنصر الثقة محوراً أساسياً فيها (كمهنة الطب أو المحاماة أو تدقيق الحسابات).

نرى أن الجريمتين محل البحث وإن اتفقنا في العلة التشريعية وهي (حماية البيانات والمعلومات المتعلقة بالأشخاص الطبيعيين) إلا أنهما تختلفان في الموضوع أو المحل، وبناء عليه، يمكن القول أن النصوص التقليدية لجريمة "إفشاء الأسرار لا تصلح لحماية البيانات "الاسمية" التي تكون محلاً للمعالجة الآلية والتي قد يترتب على الاعتداء عليها بأية صورة كانت انتهاك الحياة الخاصة والحريات الفردية. لذلك فإن مشرعنا الجزائي مطالب بالتدخل بهدف

"حماية بنوك المعلومات"، وتوفر عنصر الحماية التشريعية الجزائية من أخطاء الاعتداء على البيانات الاسمية المعالجة آليا.

بالتطرق لمسألة مهمة تتعلق– بالحرية الفردية للأشخاص؟ ألا وهي "مسألة إفشاء البيانات الاسمية بين دوائر الدولة"، لقد أنقسم الفقه الجزائي بين مؤيد ومعارض حول هذه المسألة:

فمنهم من يسبغ صفة المشروعية على أنظمة دوائر الدولة في تبادل المعلومات المتعلقة بالأفراد انطلاقا من فكرة ضبط أداء الأجهزة الحكومية وتحسين مستوى الإدارة وضبط نفقات الدولة. أما الاتجاه الآخر فيعارض الفكرة جملة وتفصيلاً، ويستند في ذلك إلى التخوف من إمكانية المساس بالحرية الشخصية للأفراد واستغلال المقارنة بين البيانات لتحقيق أغراض غير تلك التي أعلن عنها، والتي تمثل في نهاية المطاف عدواناً على الحياة الخاصة للأفراد.

وفي حقيقة الأمر فإن فكرة المساس بالحياة الخاصة للأفراد لا تتحقق إلا إذا توافرت في عملية المقارن بين البيانات المتعلقة بالشخص الواحد شروط متعددة أهمها[126]:

1. أن تكون المعلومات المخزنة في حواسيب الجهات الحكومية ذات طبيعة خاصة وعلى قدر كبير من السرية.
2. أن يكون الكشف عن هذه المعلومات غير ضروري أو متعارضاً مع الغرض الأساسي الذي أعدت من أجله.
3. أن تكون هذه المعلومات قد أعطيت بناء على التزام قانوني أو تم الحصول عليها بمراقبة الخصوصيات.

وفي المملكة الأردنية الهاشمية، وبالنظر إلى نص المادتين (21–23) من قانون الاتصالات رقم (13) لسنة (1995) اللتين تجيزان للوزارات والدوائر الحكومية والمؤسسات العامة إنشاء وتشغيل شبكات ربط واتصال خاصة لها، وربطها ببعضها البعض، فأننا نرى أنه وان كان

([126]) نصت المادة (355) من قانون العقوبات الأردني على أن يعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من: 1. حصل بحكم وظيفته أو مركزه على أسرار رسمية وأباح هذه الأسرار لمن ليس له صلاحية الاطلاع عليها .... 2. كان يقوم بوظيفة رسمية أو حكومية واستبقى بحيازته وثائق سرية ....3. كان بحكم مهنته على علم بسر وأفشاه دون سبب مشروع.

لا بد من السماح للمقارنة بين هذه البيانات بين دوائر الدولة المختلفة، إلا أن ذلك يجب أن يتم في نطاق ضيق جداً وبهدف تحقيق المصلحة العامة أولا وأخيرا لما ينطوي عليه ذلك من تهديد للحريات الشخصية للأفراد.

ومن الجدير ذكره في هذا المجال أننا نرى وجوب مراجعة تشريعاتنا الوطنية في هذا المجال حرصاً على إيجاد قوانين تضمن حماية الحياة الخاصة من المخاطر التي قد تنجم عن استعمال المعلوماتية على غرار المشرع الفرنسي الذي أوجد قانوناً عصرياً يتلاءم مع حاجات الإنسان في هذا العصر.

المبحث الثاني

الجرائم الواقعة بواسطة الحاسوب

من الجرائم التي تقع بواسطة الحاسوب الجرائم بواسطة بطاقة الائتمان:

المطلب الأول

الاستغلال غير المشروع لبطاقات الائتمان

تعد بطاقة الائتمان وسيلة متطورة بين أيدي الأفراد تستخدم أداة فنية يمكن من خلالها القيام بالوفاء أو الإيداع وهي بطاقة ممغنطة خاصة بالفرد، حيث يقوم بإدخال بعض البيانات الخاصة من خلال لوحة المفاتيح وهي تستخدم لكي تقوم أجهزة الصراف الآلي بعملها التي هي عبارة عن صناديق مقفلة بغض النظر عن حجمها والتي تشبه بالغرفة المغلقة.

وتمنح بطاقة الائتمان من البنك إلى العميل حيث يسحب ما يريد بسقف أدنى وسقف أعلى ويتم السداد شهريا، ويرسل للعميل مقدار السحب إما يدفعها مرة واحدة أو على أقساط بفوائد، سهلت بطاقات الائتمان أمور الحياة حيث تعطى من البنك للعميل كضمان على مبلغ يمكن سحبه من الصراف الآلي حتى لو كان الصندوق مغلق مما يزيد الثقة مابين البنك والعميل ويحدد البنك الصلاحيات التي تعطى للعميل في هذه البطاقة.

بطاقات الائتمان التي يتم السحب فيها يمكن استغلال هذه الثقة من الناحية المعلوماتية بالاحتيال على الصراف الآلي وعلى الشبكة ومثال ذلك: اعتماد البنك على أن يقوم بالتغطية لمحامي استملاكات حيث اعتاد البنك على أن يقوم هذا العميل بإدخال حسابات كبيرة وتسديد

حساباته، ويعطيه نتيجة لذلك بطاقة ائتمان، إلا أن هذه الاستملاكات ليست باسمه فهو يحتال على البنك على أنها باسمه –وكضمان للبنك للقيام بعملية التسديد يقوم بتسجيل منزل ضمانة باسمه وفي حالة عدم التسديد يقوم البنك ببيع المنزل في المزاد وذلك قد يعرض البنك للخسارة في حال ان ما سحبه العميل أكبر من ثمن الضمان.

وتهدف بطاقات الائتمان إلى تسهيل المعاملات من حيث السرعة وبما تمثله كونها وسيلة ائتمان بدل حمل النقود فهي أكثر فاعلية وديناميكية في التعامل وخصوصا التجاري، إلا أنها مع الزمن أصبحت تستغل لتشكل نوع من أنواع الجريمة.

التكييف القانوني لبطاقات الائتمان:

وقد فسرت فكرة الصراف الآلي وبطاقة الائتمان من قبل الفقهاء بتشبيهها بالقفل والمفتاح.

نصت م (404) من قانون العقوبات الأردني على: "يعاقب بالأشغال الشاقة المؤقتة على السرقات التي تحصل في حالة من الحالتين الآتيتين:

1. في أماكن مقفلة مصانة بالجدران مأهولة كانت أم لا ومتصلة بمكان مأهول أم لا وذلك بنقب حائطها أو بتسلقة أو بكسر بابها أو شباكها أو بفتحها بآلة مخصوصة أو باستعمال مفاتيح مصطنعة.
2. بكسر أبواب الغرف أو الصناديق الحديدية أو الخزائن المقفلة الموجودة في مكان مأهول أو غير مأهول أو فتحها بآلة مخصوصة أو مفتاح مصطنع ولو لم يتصل إليها بنقب حائط أو بتسلق أو بفتح الأقفال بآلة مخصوصة أو مفتاح مصطنع.

قام المشرع بذكر العقوبة أولا ثم قام بتعديد الحالات لبيان أن كل هذه السلوكيات معاقب عليها بذات العقوبة، ويقصد بالآلة المخصوصة هي التي يكون لها استخدامات غير الفتح ولما استخدمناها للفتح أصبحت مخصوصة للفتح مثل العتلة أو المفك...، أما المفاتيح المصطنعة مفتاح مقلد ليس بالأصلي مصطنع أي مفتاح مخروط مصطنع، فالمفتاح الذي يكون مع المالك يعتبر الأصلي وخلافه يعتبر مقلداً، واستعمال المفاتيح المصطنعة أو الآلة المخصوصة يدل

على القصد الجرمي، شدد المشرع على الكيفية أي توفر القصد العام حين عدد وسائل السرقة من نقب وتسلق وتسور واستعمال آلة مخصوصة ومفتاح مصطنع.

يصف الفقهاء الصراف الآلي بأنه غرفة مقفلة والمفتاح هو البطاقة يتكون الصراف من الاسمنت والحديد ولا يمكن ان يتم كسر الصراف او تسلقه، وإن سلمنا واعتبرنا أن الصراف غرفة حديدية واستخدمنا بطاقة ائتمان هل يمكن اعتبارها مفتاحاً أو آلة مخصوصة، تحتوي على معلومات فهي بحاجة إلى رقم سري خاص بمالكها ولا قيمة لها دون هذه المعلومات ولن يستطيع دونها أخذ المال، وفي القانون الجنائي أو توسيع النص أو تحميله أكثر مما يحتاج. وفي التجارة الإلكترونية يمكن تحويل حسابات من حساب لآخر دون البطاقة. نستنتج من ذلك أن المادة (404) لا ينطبق عليها وصف بطاقات الائتمان.

ويتم الاعتداء على بطاقة الائتمان في عدد من الحالات وهي:

1. تتعرض البطاقة للاعتداء من قبل صاحبها في ثلاث حالات:
   - استخدامها بعد انتهاء مدة صلاحيتها.
   - سحب مبلغ أكبر من الحد الأعلى.
   - استخدامها بعد أن يطلب البنك سحبها.
2. الاعتداء عليها من قبل شخص آخر باستخدامها.

الحالة الأولى: سحب مبالغ مالية تزيد عن مقدار الائتمان: يشكل هذا الفعل تجاوزاً قانونياً ولكن تجريمه محل خلاف كبير في القانون الأردني، واختلف الفقهاء فيما إذا كان يشكل هذا الفعل جريمة سرقة من عدمه وكانت الاتجاهات كالتالي:

- **الاتجاه الأول اعتبر سحب مبالغ مالية تزيد عن قيمة الائتمان لا تشكل جريمة سرقة حسب القانون الأردني**[127]، حيث لا تتوافر في هذه الحالة أركان السرقة من فعل الأخذ لأن

([127]) المادة 399 من قانون العقوبات الأردني تنص على أن: "

1. السرقة هي أخذ مال الغير المنقول دون رضاه
2. وتعني عبارة (أخذ المال) إزالة تصرف المالك فيه برفعه من مكانه ونقله وإذا كان متصلا بغير منقول فبفصله عنه فصلا تاما ونقله.
3. وتشمل لفظة مال القوة المحرزة غير الملموسة الكامنة".

التسليم في الركن المادي تم بناء على رضا البنك للعميل وتسليمه البطاقة فالسرقة قد تقع على جسم البطاقة لكنها لا تقع على قيمة الائتمان بواسطة البطاقة فلا يتم نقل الحيازة، كما أن الركن المعنوي بعنصريه العلم والإرادة أو القصد الخاص بنية التملك غير موجودة أصلا فهو صاحب البطاقة وهي ممنوحة له.

– **الاتجاه الثاني اعتبر سحب مبالغ مالية تزيد عن قيمة الائتمان إساءة ائتمان،** وذلك بالأخذ بالمادة 422[128] حيث أركان جريمة إساءة الائتمان محل الجريمة مال مادي منقول مملوك للغير سلم بموجب عقد من عقود الأمانة، فعندما يقوم العميل بفتح حساب في بنك معين يوقع على بعض الأوراق لفتح الحساب والحصول على رقم سري وبطاقة ائتمان وهذا يعد عقد من عقود الأمانة، وعندما يسحب نقود أكثر مما هو متوفر في حسابه نكون أمام إساءة ائتمان.

مثال ذلك قيام موظف بسحب أرصدة في أحد البنوك وقام بنقل من الحسابات الأرقام الصغيرة وتحويلها باسمه ولحسابه وهذه إساءة ائتمان؛ لأن الموظف له الاطلاع على الأرصدة بحكم وظيفته في عقد أمانة بينه وبين البنك فهي بالنسبة للبنك إساءة ائتمان أما بالنسبة للعملاء فهي سرقة التي هي أخذ المال المنقول بالفصل والنقل ووضعه في حيازة السارق. وفي إساءة الائتمان تحول المبالغ فيها عبر الحاسوب لذلك نلجأ للمادة 38 من قانون المعاملات الإلكترونية[129].

([128]) المادة 422 من قانون العقوبات الأردني "كل من سلم إليه على سبيل الأمانة أو الوكالة ولأجل الإبراز أو لأجل الاستعمال على صورة معينة أو لأجل الحفظ أو لإجراء عمل بأجر أو بدون أجر ما كان لغيره من أموال ونقود وأشياء وأي سند يتضمن تعها أو إبراء وبالجملة كل من وجد في يده شيء من هذا القبيل فكتمه أو بدله أو تصرف به تصرف المالك أو أستهلكه أو قدم على فعل يعد تعديا أو امتنع عن تسليه لمن يلزم تسليمه إليه يعاقب بالحبس من شهرين إلى سنتين وبالغرامة من عشرة دنانير إلى مئة دينار".

([129]) المادة 38 من قانون المعاملات الالكترونية" يعاقب كل من يرتكب فعلا يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الالكترونية بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنة أو بغرامة لا تقل عن ثلاثة آلاف دينار ولا تزيد على عشرة آلاف دينار أو بكلتا هاتين العقوبتين، ويعاقب بالعقوبة الأشد إذا كانت العقوبة المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون".

الفصل الثالث

جرائم الانترنت

سيتم التطرق بشكل من التفصيل للجرائم المرتكبة في أثناء استخدام الانترنت.حيث يلزم أن يكون النشاط التقني في مجال ارتكاب جرائم الحاسوب والانترنت مؤهلا بذاته لارتكاب الجريمة فيقوم مرتكب الجريمة بتجهيز الحاسوب ليحقق الجريمة، فقد يحتاج إلى تحميل الحاسوب ببرمجيات اختراق أو أن يقوم بإعدادها وقد يحتاج إلى تهيئة صفحات دعارة أطفال قبل الولوج إلى الانترنت وتحميلها على الخادم المضيف، أو تأهيل الحاسوب للتعامل مع فايروسات الانترنت في جريمة بث الفايروسات فيعد مرتكب هذه الجريمة من تمهيدية وتفصيلية في إعداد الفايروس أو الدودة أو القنبلة الزمنية أو حصان طروادة فالاستخدام هنا يبدو كما لو كان محددا فيه الجريمة ونظامها حيث يعد مرتكب الجريمة العمل الإجرامي والنظام الذي يعمل به لكي يحقق له النتيجة الاجرامية المبتغاه(130).

المبحث الأول

جرائم الاعتداء على الأشخاص عبر الانترنت

يمثل الانترنت بيئة خصبة للاعتداء على الأشخاص فمن خلاله تتم ممارسة العديد من السلوكيات التي تعد جرائم فيها اعتداء على قيمة وكرامة الانسان.

المطلب الأول

جرائم القدح والذم والتحقير عبر الانترنت

تعمل هذه المواقع على إبراز سلبيات الشخص المستهدف ونشر أسراره التي قد يتم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه، أو بتلفيق الأخبار عنه، وهناك

---

(130) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، جامعة عين شمس– كلية الحقوق، 2004، ص263.

حادثة مشهورة جرى تداولها بين مستخدمي الانترنت في بداية دخول الخدمة للمنطقة حيث قام شخص في دولة خليجية بإنشاء موقع ونشر صور إحدى الفتيات وهي عارية وفي أوضاع مخلة مع صديقها، وقد حصل على تلك الصور بعد التسلل إلى حاسبها الشخصي وحاول ابتزازها جنسيا ورفضت فهددها بنشر تلك الصور على الانترنت وفعلا قام بتنفيذ تهديده بإنشاء الموقع ومن ثم وزع الرابط لذلك الموقع على العديد من المنتديات والقوائم البريدية وأدى ذلك إلى انتحار الفتاة حيث فضحها بين ذويها ومعارفها[131].

وقعت حادثة تشهير أخرى ممَّن سموا أنفسهم "الامجاد هكرز" حيث أصدروا بياناً نشر على الانترنت بواسطة البريد الالكتروني ووصل العديد من مشتركي الانترنت أوضحوا فيه قيام شخص يكنى بحجازي نادي الفكر على التطاول في إحدى المنتديات بالقدح والسب السافر على شيخ الإسلام ابن تيمية والشيخ محمد بن عبد الوهاب وغيرهم من رموز الدعوة السلفية وقد استطاع الأمجاد هكرز اختراق البريد الالكتروني الشخصي للمذكور ومن ثم تم نشر صوره وكشف اسراره في موقعهم على الانترنت حيث خصصوا صفحة خاصة للتشهير به وعنوانها على الشبكة هو: http://216.169.120.174./hijazi.htm موقع منتدى الفوائد، 1421هـ.

وحوادث التشهير والقذف في شبكة الانترنت كثيرة فقد وجد ضعفاء النفوس في شبكة الانترنت وفي ظل غياب الضوابط النظامية والجهات المسئولة عن متابعة السلبيات التي تحدث في أثناء استخدام الانترنت متنفسا لأحقادهم ومرتعا لشهواتهم المريضة دون رادع أو خوف من المحاسبة وقد قيل قديما "من أمن العقوبة أساء الأدب".

تم تعريف القدح والذم في المادة 188 من قانون العقوبات حيث، "-**الذم:** هو اسناد مادة معينة إلى شخص ولو في معرض الشك والاستفهام – من شأنها أن تنال من شرفه أو وكرامته أو تعرضه إلى بغض الناس واحتقارهم سواء أكانت تلك المادة جريمة تستلزم العقاب أم لا.

([131]) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com

-**القدح:** هو الاعتداء على كرامة الغير أو شرفه أو اعتباره ولو في معرض الشك والاستفهام من دون بيان مادة معينة".

كما نصت المادة 189 "لكي يستلزم القدح أو الذم العقاب يشترط في أن يقع على صورة من الصور الآتية:

1. الذم أو القدح الوجاهي، ويشترط أن يقع:

أ. في مجلس في مواجهة المعتدى عليه.

ب. في مكان يمكن لأشخاص آخرين أن يسمعوه، قل عددهم أو كثر.

2. الذم أو القدح الغيابي، وشرطه أن يقع أثناء الاجتماع بأشخاص كثيرين مجتمعين أو منفردين.

3. الذم أو القدح الخطي، وشرطه أن يقع:

أ. بما ينشر ويذاع بين الناسأو بما يوزع على فئة منهم من الكتابات أو الرسوم أو الصور الاستهزائية أو مسودات الرسوم.

ب. بما يرسل إلى المعتدى عليه من المكتتيب المفتوحة (غير المغلقة) وبطاقات البريد.

4. الذم أو القدح بواسطة المطبوعات وشريطة أن يقع:

أ. بواسطة الجرائد والصحف اليومية أو الموقوتة.

ب. أي نوع كان من المطبوعات ووسائط النشر ".

أما المادة 190 نصت على " التحقير هو كل تحقير أو سباب -غير الذم والقدح- يوجه إلى المعتدى عليه وجها لوجه بالكلام أو الحركات أو بكتابة أو رسم لم يجعلا علنيين أو بمخابرة برقية أو هاتفية أو بمعاملة غليظة"

فهل تنطبق هذه المواد على جريمة الذم والقدح والتحقير عبر الانترنت؟ بالتمعن بالنصوص السابقة نجد أنها تستوعب ما يستجد من حالات النشر، وهناك نص خاص في المادة 38 من قانون المعاملات الالكترونية لأن هذه الجريمة تمت عبر وسائل إلكترونية، ونتمنى على

المشرع الأردني وضع نصوص جديدة تعالج هذا الموضوع أو تعديل النصوص بإضافة أو وسيلة إلكترونية إلى الوسائل الأخرى المذكورة.

المطلب الثاني

جرائم إفساد الأخلاق عبر الانترنت

تشمل الجرائم الجنسية والممارسات غير الأخلاقية المواقع والقوائم البريدية الإباحية ويندرج تحت هذا البند جرائم ارتياد المواقع الإباحية الشراء منها أو الاشتراك بها أو إنشائها التي تشكل قضية عالمية، وأما القوائم البريدية فتخصص لتبادل الصور والأفلام الجنسية على عناوينهم البريدية مجانا وتكون بعيدة عن المتابعة الأمنية، أما المواقع الإباحية يكون الهدف منها الربح المادي ويستوجب على متصفحها دفع المال مقابل الاستفادة من خدمات هذه المواقع ويتطلب كلاهما الاتصال المباشر بشبكة الانترنت، وتتيح شبكة الانترنت أفضل الوسائل لتوزيع الصور الفاضحة والافلام الخليعة بشكل علني فاضح يقتحم على الجميع بيوتهم ومكاتبهم وكل مستخدم للانترنت معرض للتأثر بما يتم عرضه على الانترنت الذي لا يعترف بأي حدود مما يشكل خطراً حقيقياً للأطفال فضلا عن الكبار نتيجة تأثيراته المؤذية وغير المرغوبة، ويوجد على الانترنت آلاف المواقع الإباحية وعدد كبير جدا من القوائم الجنسية التي أصبحت أكثر تخصصا فهناك قوائم خاصة للشواذ من الجنسين وهناك قوائم أخرى تصنف تحت دول محددة ومن المؤسف وجود بعض المواقع الشاذة بمسميات عربية والأمر أن يربط بين القوائم الاباحية والاسلام كموقع أسمى نفسه "السحاقيات المسلمات" وهكذا[132].

أصبح الانتشار الواسع للصور والأفلام الإباحية على شبكة الانترنت يشكل قضية ذات اهتمام عالمي في الوقت الراهن بسبب الازدياد الهائل في أعداد مستخدمي الانترنت حول العالم، ويندرج تحت بند المواقع والقوائم البريدية الإباحية جرائم ارتياد المواقع الإباحية سواء كان الشراء

---

(132) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com

منها أو الاشتراك فيها أو إنشاءَها، وتختلف المواقع الإباحية عن القوائم البريدية التي تخصص لتبادل الصور والأفلام الجنسية في أن المواقع الإباحية غالبا ما يكون الهدف منها الربح المادي حيث يستوجب على متصفح هذه المواقع دفع مبلغ مقطوع مقابل مشاهدة فيلم لوقت محدد أو دفع اشتراك شهري أو سنوي مقابل الاستفادة من خدمات هذه المواقع، وإن كانت بعض هذه المواقع تحاول استدراج مرتاديها بتقديم خدمة إرسال صور جنسية مجانية يوميا على عناوينهم البريدية، وأن تصفح الموقع يتطلب أيضاً الاتصال المباشر بشبكة الانترنت مما يعني أنه قد يتم حجبه.

أما القوائم البريدية فهي أسهل إنشاء وغالبا مجانية ويقوم أعضائها من المشتركين بتبادل الصور والأفلام على عناوينهم البريدية وربما تكون القوائم البريدية أبعد عن إمكانية المتابعة الأمنية حيث يركز نشاطها على الرسائل البريدية التي تكون من الصعوبة بمكان منعها من أعضاء أي مجموعة حتى وإن تم الانتباه إلى تلك القائمة لاحقا وتم حجبها فإن الحجب يكون قاصرا على المشتركين الجدد الذين لا يتوفر لديهم وسائل تجاوز المرشحات، أما الأعضاء السابقين فلا حاجة لهم إلى الدخول إلى موقع القائمة حيث يصل إلى بريدهم ما يريدونه دون أن تستطيع وسائل الحجب التدخل ويشترك في القوائم البريدية آلاف الأشخاص التي تصل أي رسالة يرسلها مشترك منهم الى جميع المشتركين مما يعني كم هائل من الرسائل والصور الجنسية التي يتبادلها مشتركي القائمة بشكل يومي.

واستفادت هذه المواقع والقوائم من الانتشار الواسع للشبكة والمزايا الاخرى التي تقدمها حيث تتيح شبكة الانترنت أفضل الوسائل لتوزيع الصور والافلام الاباحية بشكل علني يقتحم على الجميع بيوتهم ومكاتبهم، فهناك على الشبكة طوفان هائل من هذه الصور والمقالات والافلام الفاضحة بشكل لم يسبق له مثيل في التاريخ، فكل مستخدم للإنترنت معرض للتأثر بما يتم عرضه على الانترنت الذي لا يعترف بأي حدود جغرافية أو دولية فهو يشكل خطراً حقيقياً للأطفال فضلا عن الكبار نتيجة تأثيراته المؤذية وغير المرغوبة. ويوجد على الانترنت آلاف المواقع الإباحية وعدد كبير جدا من القوائم الجنسية التي أصبحت أكثر تخصصا فهناك قوائم خاصة للشواذ من الجنسين وهناك قوائم أخرى تصنف تحت دول محددة.

كشفت إحدى الدراسات أن معدل التدفق على المواقع الإباحية في أوقات العمل التي تبدأ من الساعة التاسعة صباحا إلى الخامسة عصرا تمثل (70%) من إجمالي نسبة التدفق على تلك المواقع[133]. وبان هناك إقبالاً كبيراً جداً على المواقع الإباحية حيث تزعم شركة (playboy) الإباحية أن حوالي 5 مليون زائر يزورون صفحاتهم على الشبكة أسبوعيا وبأن بعض الصفحات الإباحية يزورها (0.5) مليون زائر يوميا وان هناك مائة صفحة مشابهة تستقبل أكثر من 20 الف زائر يوميا وأكثر من الفين صفحة مشابهة تستقبل أكثر من ثلاثة آلاف زائر يوميا، وأن صفحة واحدة من هذه الصفحات استقبلت خلال عامين (44) مليون زائر، ووجد أن (83.5%) من الصور المتداولة في المجموعات الإخبارية هي صور إباحية وبأن أكثر من (20%) من سكان أمريكا يزورون الصفحات الإباحية حيث تبدأ الزيارة غالبا بفضول وتتطور إلى إدمان وغالبا لا يتردد زوار هذه المواقع من دفع رسوم مالية لقاء تصفح المواد الإباحية بها أو شراء أفلام إباحية منها وقد بلغت مجموع مشتريات المواد الإباحية في الانترنت في عام (1999م) ما نسبته (8%) من دخل التجارة الالكترونية البالغ (18) مليار دولار ووصل إلى (3) مليار دولار في عام 2003.

وتمثل الصفحات الإباحية أكثر صفحات الانترنت بحثا وطلبا كما أوضحت دراسة أجريت عام 1999 أن المواقع الإباحية أصبحت مشكلة حقيقية وأن الآثار المدمرة لهذه المواقع لا تقتصر على مجتمع دون الآخر ويمكن أن يلمس آثارها السيئة على ارتفاع جرائم الاغتصاب بصفة عامة واغتصاب الأطفال بصفة خاصة والعنف الجنسي وفقد العائلة لقيمها ومبادئها وتغيير الشعور نحو النساء إلى الابتذال بدل الاحترام. ويبدو ان لكثرة المواقع الاباحية على الانترنت التي يقدر عددها بحوالي 70 الف موقع دوراً كبيراً في إدمان مستخدمي الانترنت عليها

---

(133) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com

Dolf Zillman and Jennings Bryant, “Pornography, Sexual Callousness, and the Trivialization of Rape, “Journal of Communications 32, 1982

حيث اتضح أن نسبة 15% من مستخدمي الانرتنت البالغ عددهم (10) ملايين شخص تصفحوا المواقع الإباحية في شهر إبريل عام 1998م.

وقد جرى حصر القوائم العربية الإباحية فقط دون القوائم الأجنبية في بعض المواقع على شبكة الانترنت ومنها مواقع (yahoo) فوجد انها تصل إلى 171 قائمة باغ عدد أعضاء أقل تلك القوائم 3 في حين وصل أكثرها أعضاء إلى 9 آلاف، وتعتبر الإباحية الخلقية والدعارة من التجارة الرائجة، فقد ذكرت وزارة العدل الأمريكية قي دراسة لها[134]، أن تجارة الدعارة والإباحية الخلقية تجارة رائجة جدا يبلغ رأس مالها ثمانية مليار دولار ولها أواصر وثيقة تربطها بالجريمة المنظمة، وأن تجارة الدعارة هذه تشمل وسائل عديدة كالكتب والمجلات وأشرطة الفيديو والقنوات الفضائية الإباحية والانترنت وتفيد الإحصاءات الاستخبارات الأمريكية (FBI) أن تجارة الدعارة هي ثالث أكبر مصدر دخل للجريمة المنظمة بعد المخدرات والقمار[135]، حيث أن بأيديهم 85% من أرباح المجلات والأفلام الإباحية.

أثر الإباحية في إنحطاط القيم وتفشي الإجرام:

وجد عالم النفس (إدوارد دونرستين) من جامعة (وسكونسون) بامريكا أن الذين يخوضون في الدعارة والغباحية غالبا ما يؤثر ذلك في سلوكهم من زيادة في العنف وعدم الاكتراث لمصائب الآخرين وتقبل لجرائم الاغتصاب، ووجد عدد من الباحثين أن مثل هذه الإباحية تورث جرائم الاغتصاب، وإرغام الآخرين على الفاحشة، وهواجس النفس باغتصاب الآخرين وعدم المبالاة لجرائم الاغتصاب وتحقير هذه الجرائم[136].

---

(134) Report of the Attorney General's Task Force on Family Violence, U.S. Department of Justice, Washington, D. C.

(135) Federal Bureau of Investigation, reported in "Talking Points: Important Facts About Pornography, Take Action Manual ,National Coalition for the protection of Children and Families, p. 8

(136) Edward Donnerstein, "Pornography: Its Effects on Violence Against Women" in Malamuth and Donnerstein, eds., Pornography and Sexual Aggression, Academic Press, 1984

ولقد قام الباحث الكندي (جيمز شك) بدراسة عدد من الرجال الذين تعرضوا لمصادر مواد إباحية بعضها مقترنة بالعنف وبعضها لا تختلط بعنف، وكانت نتيجة هذه الدراسة وجد هذا الباحث أن النتيجة واحدة في كلتا الحالتين ووجد تأثيرا ملحوظا في مبادئهم وسلوكهم وتقبلهم بعد ذلك لاستعمال العنف لإشباع غرائزهم(137). ولقد وجد الباحثان (دولف زيلمان و جينينجز براينت) أن من أكثر تداول هذه المواد أصبح لا يرى أن الاغتصاب جريمة جنائية ولاحظ هذان الباحثان على هؤلاء الشاذين الإدمان والانحطاط والتدني والشغف بما هو أشنع وأبشع من ناحية الإباحية الأخلاقية كالاغتصاب وتعذيب المغتصبين واللواط وتعذيب الأطفال وفعل الفاحشة بالجمادات والحيوانات وفعل الفاحشة بالمحارم وغير ذلك(138).

ويؤكد هذه الحقيقة بحث أجراه الباحثون (الزابيث باولوتشي ومارك جينيوس وكلوديو فايولاتو) في كندا حيث أقاموا بدراسة 74 بحثا مختلفا كلها تدرس تأثير المواد الاباحية الجنسية على الجرائم الجنسية بشتى أنواعها، ولقد شملت هذه الدراسات عددا من الدول الصناعية مثل اميركا وكندا ودول أوروبا ما بين السنوات 1953 و1997م تشمل في مجموعها دراسة (13) الف شخص قد تعرضوا لمثل هذه المواد، كان من نتائج هذا البحث أن نسبة الانحطاط الخلقي العام (حسب معايير الغرب) هي 28% (وتشمل التعري، والتجسس على أعراض الآخرين بالكاميرات الخفية، والاحتكاك الجسماني بالآخرين في الأماكن المزدحمة، الخ) كما وجدوا أن نسبة الازدياد في جرائم العنف والاغتصاب تزداد عند متداولي المواد الإباحية بنسبة 30%. وإن نسبة الانحطاط في العلاقات الزوجية والقدرة الجنسية مع الزوجة تتدنى بنسبة 32% ونسبة تقبل جرائم الاغتصاب وعدم المبالاة بها تزداد بنسبة 31%(139).

---

(137) James Check, "The Effects of Violent and Nonviolent Pornography", Department of Justice, Ottawa Canada, submitted June 1984

(138) Dolf Zillman and Jennings Bryant, "Pornography, Sexual Callousness, and the Trivialization of Rape, "Journal of Communications 32, 1982

(139) Elizabeth Oddone Paolucci, Mark L. Genuis, and Claudio Violato, "The Effects of Pornography on Attitudes and Behaviours in Sexual and Intimate Relationships, "National Foundation for Family Research and Education (NFFRE), 2000

والذين يروجون الوسائل الإباحية غالبا ما تكون لهم علاقات وطيدة بالجريمة المنظمة كما يدعون إلى تفشي جرائم أخرى فمؤسسة (playboy) تدعو منذ 1966 إلى إباحة المخدرات[140]. وقد بدأت المؤسسة منذ عام 1971 بالتبرع سنويا بمبالغ لا تقل عن 100 ألف دولار لإلغاء قوانين منع المخدرات[141]، وتصدر هذه المؤسسة سنويا عددا من المقالات التي تدعو الناس إلى نصرتهم في تلك المساعي.

وتفيد الاحصاءات أن 33% من ضحايا الاغتصاب يفكرون بالانتحار أو ينتحرون[142]، والذين يدمنون المواد الإباحية غالبا ما تصبح أحوالهم مثل مدمني المخدرات والمسكرات، فبعد حين من الزمن فإنهم يجدون أنهم لا يتمالكون أنفسهم أمام هذا البلاء وهم على استعداد لافناء أموالهم من أجل إشباع غرائهم.

المطلب الثالث

جرائم الاستغلال الجنسي للأطفال عبر الانترنت

في دراسة أجراها الدكتور مشعل القدهي اتضح أن أكثر مستخدمي المواد الإباحية تتراوح أعمارهم مابين (12) و (15) عام، وأضحت دراسة أجرتها أدست (Adsit) أن المواقع الإباحية أصبحت مشكلة حقيقية وأن الآثار المدمرة لهذه المواقع لا تقتصر على مجتمع دون آخر ويمكن لمس آثارها السيئة على ارتفاع جرائم الاغتصاب بصفة عامة واغتصاب الأطفال بصفة خاصة، العنف الجنسي، فقد العائلة لقيمها ومبادئها وتغير الشعور نحو النساء إلى الابتذال بدل الاحترام[143].

---

(140) Dr. Judith Reisman, the presiden of Washington's Institute for Media Education.

(141) "American Drugs Culture Has Roots in Playboy. " National Federation for Decency Journal, November/Desember 1986, page4

(142) Kilpatrick et. Al. Rape in America:" A Report to the Nation, "April 23, 1992, p.7

(143) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com

أما بالنسبة لجريمة اغتصاب الأطفال فلقد وجد بعد دراسة 1400 حالة من هذا النوع في مدينة (لويسفيل) مابين السنوات 1980 و 1984م أن صورا عارية للبالغين متواجدة عند جميع هؤلاء المجرمين وصورا خليعة للأطفال موجودة عند أغلبهم[144].

قالت منظمة خيرية معنية بشؤون الطفل أن جرائم الجنس ضد الاطفال تزايدت 15 مرة منذ عام 1988 وأن الانترنت المتاح على الهواتف المحمولة التي تتمتع بامكانيات تصوير الفيديو قد يزيد الأمر سوءا، إن شبكة الانترنت مسؤولة إلى حد كبير عن الارتفاع الهائل في جرائم الاباحية ضد الأطفال[145]، وشهد عام 2002م، 549 جريمة جنسية ضد الاطفال مقابل 35 جريمة عام 1988، ويستغل مرتكبو جرائم الجنس صعوبة تحديد هوياتهم على الانترنت لافتراس الاطفال لكن الشرطة تمكنت من تعقب بعضهم وأجهزة الكمبيوتر الشخصية الخاصة بهم.

([144]) Testimony by John B. Rabun, deputy director, National Center for Missing and Exploited Children, before the subcommittee on Juvenile Justice of the Senate Judiciary Committee, 12 September 1984

([145]) تقرير لمنظمة ناشيونال تشايلدز هوم – تحمل حاليا اسم ان سي اتش.

المبحث الثاني

جرائم الاعتداء على الأموال عبر الانترنت

تشمل جرائم السطو على أرقام البطاقات الائتمانية، لعب القمار، التزوير، الجريمة المنظمة، المخدرات، وغسيل الأموال، ومن المعروف أن هذه الجرائم مجرمة حيث لا تختلف في نتيجتها عن الجرائم التقليدية التي تحمل نفس المسمى.

المطلب الأول

التحويل الإلكتروني غير المشروع للأموال

1. **جرائم السطو على أرقام البطاقات الائتمانية:** بعد انتشار مفهوم التجارة الالكترونية في السبعينات استفادت من مزاياها الكثير من شركات الاعمال وأصبح من السهل الاستيلاء على بطاقات الائتمان وتم سرقة مئات الالوف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنت ومن ثم بيع هذه المعلومات للآخرين، ويتعدى الامر المخاطر الأمنية التي تتعرض لها بطاقات الائتمان فنحن في بداية ثورة نقدية تعرف باسم النقود الالكترونية التي يتنبأ لها أن تكون مكملة للنقود الورقية، وأن هناك الأسهم والسندات الالكترونية المعمول بها في دول الاتحاد الاوروبي التي أقر الكونجرس الأمريكي التعامل بها عام 1990 فالتعامل معها من خلال الانترنت سيواجه مخاطر أمنية ولا شك[146].

2. **القمار عبر الانترنت:** تتداخل عملية غسيل الأموال مع أندية القمار المنتشرة، الأمر الذي جعل مواقع الكازينوهات الافتراضية على الانترنت محل اشتباه ومراقبة من قبل السلطات الامريكية، وعلى الرغم من أن سوق القمار في امريكا يعدّ الأسرع نموا على الاطلاق إلا أن مواقع القمار الافتراضية على الانترنت غير مصرح بها ويلجأ بعض أصحاب تلك المواقع إلى إنشائها وإدارتها من أماكن مجاورة لأمريكا. ويوجد على الانترنت أكثر من ألف موقع للقمار

([146]) عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، الكتاب الاول، درا الفكر الجامعي، الازاريطة – الاسكندرية، ص106 وما بعدها.

يسمح لمرتاديه من مستخدمي الانترنت ممارسة جميع انواع القمار التي تمارسها المواقع الحقيقية[147].

3. **تزوير البيانات:** تتم عملية التزوير بالدخول إلى قاعدة البيانات وتعديل البيانات الموجودة بها على أو إضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك، وفي حادثة وقعت في ولاية كاليفورنيا الأمريكية عمدت مدخلة بيانات بنادي السيارات وبناء لاتفاقية مسبقة بتغيير ملكية السيارات المسجلة في الحاسب الآلي لتصبح باسم أحد لصوص السيارات وبدوره يعمد إلى سرقة السيارة وبيعها وعندما يتقدم مالك السيارة للإبلاغ يتضح عدم وجود سجلات للسيارة باسمه وبعد بيع السيارة تعاود الفتاة تسجيل السيارة باسم مالكها وتتقاضى مقابل ذلك مبلغ مائة دولار.

المطلب الثاني

جريمة إتلاف نظم المعلومات

وتشمل جرائم تدمير المواقع، واختراق المواقع الرسمية أو الشخصية، اختراق الأجهزة الشخصية، اختراق البريد الالكتروني للآخرين أو الاستيلاء عليه أو إغراقه والاستيلاء على اشتراكات الآخرين وأرقامهم السرية وإرسال الفيروسات، جميع هذه الجرائم تبدأ بانتهاك خصوصية الشخص، وهذا سبب كافٍ لتجريمها فضلا عن إلحاق الضرر المادي والمعنوي بالمجني عليهم.

1. **الاقتحام أو التسلل:** وتشمل الاختراقات سواء للمواقع الرسمية أو الشخصية أو اختراق الأجهزة الشخصية، اختراق البريد الإلكتروني أو الاستيلاء عليه والاستيلاء على اشتراكات الآخرين وأرقامهم السرية، ولكي يتم الاختراق يستخدم المتسللون ما يعرف بحصان طروادة وهو برنامج صغير يتم تشغيله داخل جهاز الحاسب لكي يقوم بأغراض التجسس على أعمال الشخص الذي يقوم بها على حاسوبه الشخصي فهو في أبسط صورة يقوم بتسجيل كل طرقة قام

([147]) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com

بها على لوحة المفاتيح منذ أول لحظة للتشغيل ويشمل ذلك كل بياناته السرية أو حساباته المالية أو محادثاته الخاصة على الانترنت أو رقم بطاقة الائتمان الخاصة به أو حتى كلمات المرور التي يستخدمها لدخول الانترنت التي قد يتم استخدامها بعد ذلك من الجاسوس الذي قام بوضع البرنامج على الحاسب الشخصي للضحية[148].

ويعدُّ الهجوم على المواقع المختلفة في شبكة الانترنت من الجرائم الشائعة في العالم وقد تعرضت لهذا النوع من الجرائم في الولايات المتحدة مثلا كل من وزارة العدل والمخابرات المركزية والقوات الجوية كما تعرض له حزب العمال البريطاني.

ولا تساعد العقوبات الحالية على تقليص الارتفاع المستمر للجرائم المتعلقة بالحاسب الآلي ففي خلال عام واحد تضاعفت تلك الجرائم على مستوى الولايات المتحدة الأمريكية عام 1999.

2. **فيروسات الحاسب الآلي:** وهي برامج تكون الأوامر المكتوبة فيها تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته، وتعرف بأنها نوع من البرامج التي تؤثر في البرامج الأخرى بحيث تعدل في تلك البرامج لتصبح نسخة منها وهذا يعني ببساطة أن الفايروس ينسخ نفسه من حاسوب إلى آخر بحيث يتكاثر بأعداد كبيرة[149].

وتقسم الفيروسات إلى خمسة أنواع فايروسات الجزء التشغيلي للإسطوانة، والفايروسات المتطفلة، والفيروسات المتعددة الانواع، الفايروسات المصاحبة للبرامج التشغيلية، وحصان طروادة حيث يختفي الفايروس عن البرامج المضادة للفيروسات إلا أن أثره التدميري خطير[150].

بعض هذه الفيروسات لها أسماء طريفة مثل Darken Avenger و Christmas Card و Monkeys هذا مع العلم بأن عددها قد تجاوز الثلاثة آلاف فيروس، ومن هذه الوسائل المعتمدة لإتلاف المعلومات القنبلة المعلوماتيه وهي نوع من الفيروسات وتقوم بتدمير المعلومات.

---

(148) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com

(149) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، المرجع السابق.

(150) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com

أما عند حدوث ظرف معين مثل شطب اسم احدهم من قائمة المستخدمين في الشركة وهي ما يعرف بالقنبلة المنطقية وإما في ساعة محددة بتاريخ محدد وهي ما تعرف بالقنبلة الزمنية، ومن هذه الوسائل أيضا الدودة وهي عبارة عن برامج تستغل أية فجوات في نظم التشغيل لتنتقل من حاسب إلى آخر عبر الشبكات وتقوم بعد ذلك بالتكاثر وهي أيضا من نوع الفيروس(151).

والفيروسات وهي عبارة عن برامج تدميرية تقوم بعمل مشابه للفيروس البيولوجي وتتكاثر مثله، وهي تصيب أنظمة المعلومات وتمتلك القدرة أحيانا على تعديل البرامج الأخرى. وقد أسهم في انتشار هذه الفيروسات عملية القرصنة المعلوماتية والانتشار الواسع لشبكات المعلومات.

إن خصوصية جرائم المعلومات تستوجب وجود تشريعات خاصة؛ لأن الأحكام العامة المنصوص عليها في قوانين العقوبات قد لا تفي بالغرض لأنه ينشأ عن إجمال خصوصية هذه الجرائم عدم إمكانية معاقبة مرتكبيها هذا مع العلم بأنه في مثل هذه الحالات لا يمكن استخدام القياس للتجريم عملاً بمبدي "لا جريمة ولا عقوبة دون نص"، فكيف يمكن أن نقبل أن يبقى مرتكبو هذه الجرائم دون عقاب كما ننوه في هذا المجال بالتقدم الحاصل في التشريع اللبناني مع صدور قانون حماية الملكية الأدبية والفكرية رقم 99/75 الذي شمل بالحماية في مادته الثانية برامج الكمبيوتر وعاقب من يتعدى على حقوق مؤلفيها في الفصل الحادي عشر منه(152).

---

(151) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1–3 مايو 2000.

(152) وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1–3 مايو 2000.

الفصل الرابع

التحقيق والإثبات في جرائم الحاسوب والانترنت في المملكة الأردنية الهاشمية

أدى تزايد استخدام الأنظمة القائمة على الحاسب الآلي إلى الكشف عن العديد من المخاطر والتهديدات لهذه النظم الجديدة سواء نجمت هذه المخاطر من نظم المعلومات نفسها مثل أخطاء تشغيل النظام ذاته، أو من كوارث الطبيعة أو نتيجة سلوكيات جرميه لبعض المخربين أو المتطفلين أو معتادي الإجرام، ولذلك فإننا نصبح في حاجة ماسة إلى وضع نظام لتأمين نظم المعلومات وحمايتها من أية مخاطر أو تهديدات.

وحماية نظم المعلومات (بمكوناتها المادية وغير المادية) هي مسألة فنية تقنية بالدرجة الأولى، يهتم بها صاحب الحق المحمى، كما يهتم بها نظام العدالة الجزائية في المجتمع، باعتبار أن موضوع السياسة الجزائية هو تامين تماسك وبقاء الكيان الاجتماعي بضمان تأمين حماية الأشخاص والأموال في المجتمع، وإذا كان البعض يعتقد أن الحماية الجزائية لنظم المعلومات

(أو للمعلوماتية) يمكن أن يتحقق بمجرد سن تشريعات تعالج هذه الأنماط المستحدثة لأوضاعها الحالية، فإن تلك النظرة تعد قاصرة ما لم يأخذ بعين الاعتبار التطورات المحتملة في هذا المجال، والتي يرجح أن تتخذ شكل الطفرات أو القفزات التي لم تكن في حسبان أكثر العلماء تفاؤلا منذ سنوات قليلة مضت، وأيضا فأن الحماية الجزائية المنشودة لا بد وأن تتبع من إستراتيجية متكاملة لمكافحة جرائم الحاسوب تتناول كافة أدوار أجهزة العدالة الجزائية في المجتمع تشريعية وقضائية وتنفيذية، كما تراعى الطبيعة الخاصة لهذه وجرائم، وما يميزها من صعوبة في

التحقيق والتفتيش والإثبات وسيتم البحث في واقع جرائم الحاسوب في التشريع الجزائي الأردني بهدف التعرف على مدى كفاية النصوص العقابية الحاضرة في مواجهة تلك الجرائم[153].

إن مواجهة الجريمة المعلوماتية تواجه العديد من التحديات في مسألة استخلاص الدليل الذي تثبت به الجريمة المعلوماتية، فهناك صعوبة في جمع الاستدلالات والأدلة في الجريمة المعلوماتية حتى يمكن تحقيق عناصرها فهذه النوعية من الجرائم توجد في بيئة لا تعتمد التعاملات فيها على الوثائق والمستندات المكتوبة، وإنما على نبضات إلكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الحاسب والبيانات التي يمكن استخدامها كأدلة ضد الفاعل يمكن في أقل من الثانية محوها.

أدى ذلك إلى اتساع دور العدالة الجنائية عند ممارستها لحق المجتمع في الدفاع عنه ضد الجريمة أن تتعامل مع الأدلة غير المادية في مجالات الإثبات الجنائي، فعليها في عملية التحقيق السعي لتطوير أساليب كشف الجريمة المعلوماتية والوسائل المستخدمة في عمليات البحث الجنائي، وتطوير الأساليب الإجرائية لجمع الأدلة في الجرائم المعلوماتية.

وعلى رجال الاستدلال والتحقيق تطوير قدراتهم العلمية ليتمكنوا من التفاهم مع خبراء الحاسب الآلي وحسن استغلالهم في كشف الجرائم وجمع الأدلة، فيجب أن يكون المحقق ملم بالإجراءات الاحتياطية التي تتخذ نحو مسرح الجريمة وتأمين الأدلة.

كل ما سبق يبين أهمية القيام بالتحقيق واستخلاص الدليل في الجريمة المعلوماتية، وسيتناول هذا الفصل التحقيق والاثبات في جرائم الانترنت في المملكة الأردنية الهاشمية من خلال ثلاثة مباحث حيث يبين المبحث الأول الجهات المختصة بالقيام بعملية التحقيق في جرائم الحاسوب والانترنت.

([153]) نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1-3 مايو 2000.

أما المبحث الثاني من هذا البحث سيتناول كيفية إجراءات التحقيق الفني من حيث محل التحقيق والصعوبات المتعلقة بعملية التحقيق وصولا لعملية الضبط في بيئة الحاسب الآلي. من ثم الاثبات الجنائي في بيئة الحاسوب والانترنت في المبحث الثالث.

المبحث الأول

الجهات المختصة بالتحقيق في جرائم الحاسوب والإنترنت

تباشر النيابة العامة إجراءات التحقيق بوصفها صاحبة اختصاص أصيل بدءا بمرحلة التحقيق الابتدائي التي تهدف لجمع الأدلة المادية التي تثبت وقوع الجريمة ونسبتها إلى فاعل معين وفقا للأصول الإجرائية الواردة في القانون[154]. والدليل المادي هو الدليل المعتمد على عناصر ظاهرة محسوسة مادية يتركها الجاني خلفه في ساحة الجريمة كالشعر والدم والبصمات.. تلتقط بالتفتيش أو بأي وسيلة أخرى كالخبرة والضبط والمعاينة.

المطلب الأول

النيابة العامة كصاحبة اختصاص أصيل

إن إجراءات التحقيق تمس حقوق وحريات الأفراد لذلك حرص المشرع الجزائي على إيلائها جهة قضائية وهي النيابة العامة ممثلة بالمدعي العام كقاعدة عامة، وهناك استثناءات في قانون أصول المحاكمات الجزائية أعطيت صلاحيات التفتيش لغير المدعي العام (النيابة العامة)، وهذه الحالات هي:

أولا: الجرم المشهود:

تتسع في هذه الحالة سلطات الضابطة العدلية فتباشر اختصاصها أصلا من قبيل إجراءات التحقيق التي تثبت للمدعي العام وتحديدا البحث عن أدلة الجريمة وتحديد فاعلها، وهذه الصلاحية لا تثبت لكافة أعضاء الضابطة العدلية وإنما تقتصر على ضباط الشرطة ورؤساء

([154]) أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت –دراسة تحليلية مقارنة–، دار وائل للطباعة والنشر، عمان – الأردن، ط1، س2001، ص263.

مخافر الشرطة فلهم إجراء تفتيش المشتبه به أو مسكنه في حال وقوع جريمة من جرائم الحاسب الآلي وتوافر شروط الجرم المشهود[155].

ثانيا: الإنابة في التفتيش:

للمدعي العام أن ينيب عنه قاضي صلح أو مدعي عام أو أي عضو من أعضاء الضابطة العدلية لإجراء معاملات تحقيق، وفي حال كان المستناب قاضي صلح أو مدعي عام آخر يجوز للمدعي العام إنابته لإجراء أي من معاملات التحقيق، أما إذا كان المستناب أحد أعضاء الضابطة العدلية فله إنابته بأي معاملة من معاملات التحقيق باستثناء استجواب المشتكى عليه لخطورة هذا الاجراء ويتبع باصدار مذكرة توقيف أو إطلاق سراح المقبوض عليه وعضو الضابطة العدلية لا يملك ذلك، ويشترط أن تصدر الإنابة من مختص محددا فيها محل التفتيش ووقته[156].

ثالثا: الجرائم الواقعة داخل مسكن:

للمدعي العام ولضباط الشرطة ورؤساء مخافر الشرطة في حال وقوع جناية أو جنحة داخل مسكن صلاحيات طالما طلب إليهم صاحب المسكن إجراء التحقيق فيها، فلهم صلاحية التفتيش في حالة وقوع جريمة من جرائم الحاسب الآلي.

حيث تقوم الجهات المذكورة بالإجراءات اللازمة للحصول على الأدلة الجرمية وضبطها وكشف حقيقتها وإزالة الغموض الذي يحيط بها، وترجيح نسبتها إلى شخص معين، مثل ضبط برامج غير مشروعة على جهاز الحاسوب الخاص بالمتهم وتقديمها كدليل اتهام ضده أمام المحكمة المختصة[157].

---

(155) اسامة المناعسة وآخرون –جرائم الحاسوب والانترنت–ط1–دار وائل – عمان– 2001م، ص267.

(156) اسامة المناعسة وآخرون –جرائم الحاسوب والانترنت – ط1 –دار وائل عمان – 2001م، ص268.

(157) هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، ط1، دار النهضة العربية، القاهرة، 1997، ص 46.

فإذا تم التحقيق في مرحلة الاستدلال أي قبل تحريك الدعوى الجزائية فإنه يُعد عملاً من أعمال الاستدلال، أما إذا تم التحقيق بعد تحريك الدعوى الجزائية فإنه يُعد عملاً من أعمال التحقيق الابتدائي، وقد تضطر السلطة المختصة بالتحقيق إلى أن تقوم ببعض التحريات كالتنصت والتجسس المعلوماتي، ولا تستطيع أن تقوم بإجراء التفتيش بالسرعة اللازمة لضبط الأدلة، ويرى جانب من الفقه الغربي أن التنصت الإلكتروني مشروع، وأنه من الأفضل منح الشرطة سلطة واسعة في إجراءاتها في حالات التفتيش الطارئ[158].

فإذا قام بإجراء التفتيش مدع عام أو من ينيبه بموجب مذكرة إنابة، فإن التفتيش يُعد عملاً من أعمال التحقيق، أما إذا ما قام بإجراء التفتيش عضو ضابطة عدلية غير مخول بإجرائه بموجب مذكرة تفتيش، فإن التفتيش يُعد عملاً من أعمال الاستدلال كالتفتيش الوقائي الذي يقتصر هدفه على تجريد المقبوض عليه من شيء خطر يحمله[159].

بيّن المشرع الأردني في المادة (46) من قانون أصول المحاكمات الجزائية وظائف موظفي الضابطة العدلية في المراكز التي لا يوجد فيها مدع عام بالنص على: (أن موظفي الضابطة العدلية المذكورين في المادة (44) ملزمون في حال وقوع جرم مشهود أو حالما يطلبهم صاحب البيت أن ينظموا ورقة الضبط ويستمعوا لافادة الشهود وأن يجروا التحريات وتفتيش المنازل وسائر المعاملات التي هي في مثل هذه الأحوال من وظائف المدعي العام وذلك كله طبقاً للصيغ والقواعد المبينة في الفصل الخاص بإجراء وظائف المدعي العام). إن مثل هذا الإجراء الخطير يحتاج صدوره إلى سلطة مختصة وهي النيابة العامة.

وبناء على ما تقدم فإن التفتيش يعد إجراء من إجراءات التحقيق عندما تقوم به السلطة المختصة بالتحقيق الابتدائي، وبعد تحريك الدعوى الجزائية ومباشرتها بقصد الكشف عن الحقيقة.

([158]) علي طوالبة، رسالة دكتوراه، التفتيش الجنائي على نظم الحاسوب والانترنت– دراسة مقارنة –جامعة عمان العربية للدراسات العليا –2003م.

([159]) علي طوالبة، المرجع السابق.

أن التفتيش الواقع على مكونات الحاسوب المادية لا توجد فيه مشكلة في التنفيذ لإمكانية ذلك وسهولته مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها أو محوها بسهولة، لذا يقتضي القيام بهذا الإجراء من مختصين في مجال الحاسوب، مثال ذلك: ضبط جهاز الحاسوب نفسه أو جزء منه كالقرص الصلب أو الشاشة أو لوحة المفاتيح ...الخ، وسبب سهولة هذا التفتيش لأنه يقع على أشياء مادية منصوص عليها في أغلب القوانين الإجرائية، لكن المشكلة هي في إمكانية تفتيش وضبط مكونات الحاسوب المعنوية كالبرامج والنظم الخاصة بالتشغيل وقواعد البيانات...الخ، والتي يمكن أن تنظم جريمة ما أو تخزن طريقه ارتكاب جريمة بواسطة الحاسوب، وقد يتعذر ضبط هذا البرنامج إلا إذا اندمج مع كيان مادي كالقرص الصلب مثلا.

فقامت بعض القوانين والاتجاهات الفقهية بالتعامل مع الوضع باعتبار عدم إمكانية انسجام وتطابق أحكام التفتيش والضبط في القانون الجنائي الإجرائي مع ما قد يتطلبه كشف الحقيقة في جرائم نظم المعلومات من بحث وتنقيب عن الأدلة في برامج الحاسوب وبياناته، حدد جانب من التشريعات الإجرائية هدف التفتيش بالبحث عن شيء وضبطه كما في القانون الأردني والمصري..، وعملت الدول التي أخذت بهذا الاتجاه إلى حماية هذه الكيانات المعنوية عبر قوانين الملكية الفكرية.

وهناك من عبر عن شمول النص في بعض القوانين الإجرائية بإصدار أمر قضائي لتفتيش وضبط أي شي وتشير الدلائل أن هناك جريمة وقعت أو يشك في وقوعها. يقوم الفقه بتفسير هذه النصوص بشكل أوسع إلى حد يسمح بتفتيش وضبط الكيانات المعنوية للحاسب الآلي، ومما تقدم يخلص أصحاب هذا المسار إلى أن برامج الحاسوب يمكن أن تنطبق عليها خصائص المادة فتدخل في نطاق الأشياء المادية.

ويرى جانب من الفقه الجنائي الأردني أن قانون أصول المحاكمات الجزائية الأردني جاء بمفهوم واسع وشامل للتفتيش وغايته، عندما أعطى لسلطة التفتيش في أكثر من مادة ،صلاحيات ضبط أي (شيء) يمكن الاستدلال به على كشف الجريمة والمجرمين، وأن لفظ

(الأشياء) الوارد في نصوص قانون الأصول الأردني يمكن أن يكون شاملاً بحيث تبسط نظرية التفتيش نطاقها لتشمل مفردات الحاسوب المعنوية، عندما ترتكب في بيئة الحاسوب ضمن الشرائط القانونية[160].

يهدف التفتيش لجمع الأدلة ذات الحجية التي تثبت وقوع الجريمة وتكشف عن هوية فاعلها، ويقصد بحجية المخرجات الكمبيوترية قيمة ما يتمتع به المخرج الكمبيوتري بأنواعه المختلفة من قوة استدلالية على صدق نسبة الفعل الإجرامي إلى شخص معين أو كذبه[161]، ولكي يكون التفتيش صحيحا يجب توافر ثلاثة شروط؛ وهي وقوع جريمة ونسبتها لفاعل معين توفر الأدلة والإمارات على ذلك.

يجب أن تقع جريمة بصورة محققة للقيام بإجراءات التفتيش، سواء أكانت هذه الجريمة جنحة أو جناية، فإن لم تكن هناك جريمة فلا مجال للقيام بالتفتيش المقصود إذ لا غاية له[162]. وحسب مبدأ الشرعية (لا جريمة ولا عقوبة إلا بنص) فإن على المشرع التدخل السريع لتجريم الأفعال التي تقع في بيئة الحاسب الآلي كونها سلوكيات حديثة تعجز النصوص التقليدية عن مواكبتها وتنظيمها.

إنَّ وقوع جريمة لا يعني القيام بالتفتيش عشوائيا بل يتطلب ذلك ضوابط تتعلق بالمكان والشخص المراد تفتيشه فيقتضي الأمر أن يكون فاعلا أو شريكا في الجريمة أو مساهما فيها، حيث تتضمن مذكرة التفتيش اسم الشخص المشتبه به والمكان المراد تفتيشة والأشياء المبحوث عنها ونوع الجريمة وطبيعتها، وللمدعي العام ممثلا للنيابة العامة صلاحية إجراء التفتيش في كافة الأمكنة[163].

---

(160) اسامة المناعسة وآخرون–جرائم الحاسوب والإنترنت–ط1–دار وائل– عمان– 2001م، ص265.

(161) هلالي عبد اللاه أحمد –حجية المخرجات الكمبيوترية في المواد الجنائية –دراسة مقارنة –أسيوط– 1999م، ص22.

(162) اسامة مناعسة وآخرون– جرائم الحاسب الآلي والانترنت– ط1– دار وائل– عمان– 2001م، ص270.

(163) اسامة مناعسة وآخرون– جرائم الحاسب الآلي والانترنت– ط1– دار وائل– عمان– 2001م، ص272.

للمدعي العام أن يفتش المشتكى عليه وله أن يفتش غيره إذا اتضح من إمارات قوية أنه يخفي أشياء تفيد في كشف الحقيقة وهذا ما ورد في المادة (1/86) من قانون أصول المحاكمات الجزائية، وذلك حتى لا تكون صلا حية التفتيش وسيلة لظلم الأفراد واضطهادهم.

وإن كان قضاة التحقيق لا يقدرون الإثبات إلا من ناحية مدى كفاية الأدلة للاتهام إلا أنه لا يشترط في هذه الأدلة أن تصل إلى مرتبة اليقين التي يجب أن يبنى عليها الحكم بالإدانة، إذ يكفي لتبرير الاتهام أن تتوافر دلائل تفيد جدية الشك في ارتكاب المتهم للجريمة، فالشك يفسر ضد المتهم في مرحلة الاتهام ويفسر لصالحه في مرحلة الحكم[164].

المطلب الثاني

الضابطة العدلية واختصاصها في التحقيق

تباشر الضابطة العدلية دورا مهماً في جرائم الحاسب الآلي بدءا بمرحلة البحث الأولي وهي المرحلة الأولى من مراحل الدعوى الجزائية ومن ثم مرحلة تحريك الدعوى والتحقيق الابتدائي والتي تباشرها النيابة العامة ممثلة بالمدعي العام ومساعديه وصولا إلى مرحلة المحاكمة التي تباشرها المحكمة المختصة وفقا للقانون.

حيث أعضاء الضابطة العدلية أصحاب الاختصاص العام ويمارسون وظائفهم في جميع الجرائم، وهم:

- المدعي العام ومساعدوه، قضاة الصلح في المراكز التي لا يوجد فيها مدع عام.
- مساعدو المدعي العام، مدير الأمن العام، قواد الشرطة والدرك، الموظفون المكلفون بالتحري والمباحث الجنائية، رؤساء مخافر الشرطة والدرك، المخاتير، رؤساء المراكب البحرية والجوية.

---

(164) هلالي عبد اللاه أحمد –حجية المخرجات الكمبيوترية في المواد الجنائية –دراسة مقارنة –أسيوط– 1999م، ص41.

يوكل لأعضاء الضابطة العدلية بموجب قانون اختصاص محدود مباشرة جرائم محددة بموجب قوانينهم الخاصة، فاختصاصهم محدود، منهم:

أولا: الضابطة الجمركية: ضبط البضائع التي يثبت أن فيها اعتداء كالاعتداء على حقوق المؤلف عندما تكون البضائع برامج حاسب آلي مقلدة أو منسوخة وغيرها...

ثانيا: موظفو مكتب حماية حق المؤلف (دائرة الملكية الفكرية) فقط للمفوضين من الوزير، والجرائم المتعلقة بقانون حماية حق المؤلف.

وظائف الضابطة العدلية في الظروف العادية:

تعمل أعضاء الضابطة العدلية على استقصاء الجرائم والبحث عنها، ويشمل ذلك البحث في الركن الشرعي بالتحقق من أن الفعل المرتكب يشكل جريمة استنادا لقاعدة التكييف، والتحقق من الركن المعنوي (النية) وكذلك البحث في ظروف ارتكاب الجريمة والبحث عن الفاعل من خلال تحديد هوية المشتبه به.

وتتلقى الضابطة العدلية أيضاً الاخبارات والشكاوى بخصوص الجرائم التي تكلف بأمر بحثها واستقصائها، كما تعمل الضابطة العدلية على جمع الاستدلالات والأدلة المادية من حيث الانتقال والمعاينة وسماع الشهود واللجوء إلى الخبرة دون تحليفهم اليمين القانونية ودون أن يكون لهم سلطة إحضار من لا يريد منهم، ولهم اللجوء إلى الخبرة الفنية اللازمة لتحديد الأدلة وفي مجال الحاسب تظهر الحاجة إلى الفن والخبرة وعلى الخبير المنتدب القيام بالمهمة وليس له أن ينيب غيره بكل العمل أو بجزء منه وعليه إعداد تقريره حال الانتهاء من عمله.

وتقوم الضابطة العدلية بسؤال المشتبه به وسماع أقواله الطوعية دون إجباره، فضلاً عن تنظيم الضبوط والمحاضر، وكذلك ضبط الأوراق والأشياء الأخرى، في جرائم الحاسب الآلي يمكن إثباتها بالأدلة المعتبرة قانونا لكنها تختلف من حيث نوع الدليل وطبيعته كما يلي:

-الاعتراف، سيد الأدلة وغالب جرائم الحاسوب لا تكتشف إلا بالاعتراف أو الصدفة.

-الأدلة الورقية، سواء كان على صورة أوراق أولية تحضيرية كمسودات للعملية المراد ارتكابها.

-أوراق تجريبية لبيان مدى جاهزية الحاسب الآلي للقيام بالمهمة.

-أوراق أصلية يحتفظ بها في سجلات أصلية أساسية كمرجع لتنفيذ الجريمة.

-جهاز الحاسب الآلي وملحقاته من أجهزة إدخال وإخراج.

-الأقراص المرنة وأقراص الليزر والشرائط الممغنطة والبطاقات الممغنطة وبطاقات الائتمان والمواد البلاستيكية الخاصة المستعملة في صنع تلك البطاقات.

وتبقى الحاجة إلى الخبرة الفنية ضرورة مهمة فعند نهاية التفتيش وتحقيق غايته بالعثور على الأدلة الجرمية المبحوث عنها يتم تنظيم ضبط هذه الأدلة في بيئة الحاسب الآلي. والضبط هو وسيلة التقاط الأدلة وتثبيتها بالاعتماد على تحرير أوراق رسمية بكل خطوة تقوم بها جهة التفتيش والتقاط كل دليل معتبر في الاثبات، ويشمل الضغط كل ما استعمل في ارتكاب الجريمة وتستعين الجهة المختصة بالتفتيش والضبط باصحاب الخبرة والاختصاص في الحصول على الأدلة المكتشفة كما تستعين بكافة الوسائل اللازمة بما فيها أنظمة الحاسب الآلي[165]، مع العلم أن مكونات الحاسب المعنوية لابد لضبطها حصرها في حيز مادي لنقلها من صورتها المعنوية إلى صورتها المادية.

شروط الضبط:

1. ضرورة ضبط كل ما له علاقة بالجريمة المرتكبة والتي يمكن أن تظهر الحقيقة.
2. تنظيم الضبط من قبل مختص مكانيا وزمانيا ونوعيا وبصورة مكتوبة.
3. أن يقتصر الضبط على إثبات لواقع الحال دون زيادة أو تدخل.
4. أن يوقع المدعي العام والكاتب وكل من يشترط القانون حضوره إجراءات التفتيش والضبط على كل ورقة من أوراق الضبط بعد إطلاعه عليها.

([165]) مناعسة واخرون – جرائم الحاسب الآلي والإنترنت – ط1 – دار وائل – عمان – 2001م، ص285.

5. في حال تعذر الحضور أو الامتناع عن التوقيع يصرح بذلك في المحضر.

فيشترط في الشكل أن يكون الضبط مكتوبا ومؤرخا لتحديد الاختصاص الزماني والمكاني وموقعا لاتاحة نسبته إلى موظف معين، وكذلك يجب اشتمال الضبط على كافة الاجراءات والمعلومات والبيانات التي وجدت على مسرح الجريمة بشمول ودقة وتثبيت المعلومات المباشرة فقط والتي تكون بصورة محايدة.

وظائف الضابطة العدلية في الظروف الاستثنائية:

القبض: مع أن القبض من اختصاص سلطة التحقيق (النيابة العامة) إلا أن المشرع رأى الخروج عن ذلك للمصلحة العامة وذلك عند توافر إحدى حالات الجرم المشهود المحددة حصرا في المادة 28 بسبب:

- الجرم المشهود يقتضي بطبيعته وجود عضو الضابطة العدلية في مكان الجريمة أو مشاهدة الجرم في إحدى حالاته سواء في أثناء القيام بارتكاب الركن المادي للجريمة أو بعد ذلك عند مشاهدة آثار الجريمة.
- إعطاء صلاحيات القبض على الفاعل أمر لا بد منه لمنع فرار الفاعل مما يبعث الأمن والطمأنينة.
- ارتكاب المجرم جريمته على مرأى من الناس ينم عن عدم مبالاة واستهتار بقوة المجتمع الردعية بما يبرر توسيع صلاحيات الضابطة العدلية للقبض عليهم.

المبحث الثاني

إجراءات التحقيق الفني في جرائم الحاسوب والإنترنت

إن المحقق أو القاضي الذي يعاين جسم الجريمة سواء أكانت تقليدية أم معلوماتية عن طريق حواسه لا يمكنه معاينة الفعل الجنائي لحظة وقوعه وإنما يعاين فقط النتائج التي ترتبت عليه، وعن طريق التحليل والاستنتاج يمكنه التوصل إلى الكيفية التي تمت بها الجريمة وأداتها ومراحل تنفيذها وآثارها كما حدثت على أرض الواقع[166].

وتعد الخطوة الأهم في مكافحة جرائم الانترنت هي تحديد هذه الجرائم بداية ومن ثم تحديد الجهة التي يجب أن تتعامل مع هذه الجرائم والعمل على تأهيل منسوبيها بما يتناسب وطبيعة هذه الجرائم المستجدة، ووضع التعليمات لمكافحتها والتعامل معها والعقوبات المقترحة ومن ثم يركز على التعاون الدولي لمكافحة هذه الجرائم[167].

المطلب الأول

تحديد نوع النظام المراد التحقيق فيه

يرى جانب من الفقه الجنائي أن التحقيق الفني التقليدي يهدف إلى جمع الأدلة المادية، في حين أن نظم الحاسوب عبارة عن كيان معنوي، ولا تتوافر له صفة المادة، سواء تعلق ذلك ببرامج الحاسوب أم ما يشتمل عليه من بيانات ومعلومات ذات أهمية لمالكيها، وينتهي أصحاب هذا الرأي إلى القول بعدم إمكانية تطبيق إجراءات التحقيق الفني التقليدية على جرائم الحاسوب والإنترنت[168]، إن التطور المتزايد في استخدام الحاسب الآلي وما صاحبه من ظهور طائفة

---

[166] هلالي عبد اللاه أحمد –حجية المخرجات الكمبيوترية في المواد الجنائية –دراسة مقارنة –أسيوط– 1999م، ص80.

[167] محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com

[168] علي طوالبة، رسالة دكتوراه، التفتيش الجنائي على نظم الحاسوب والانترنت– دراسة مقارنة –جامعة عمان العربية للدراسات العليا –2003م.

جديدة من الجرائم يتطلب من السلطات القضائية أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجنائي[169].

وتوجد على الساحة القانونية ثلاثة أنظمة رئيسية للإثبات في محيط التشريعات الإجرائية المختلفة:

أولا: نظام الأدلة القانونية أو النظام المقيد: يحظر بمقتضاه أن يقيم القاضي حكمه في الدعوى إلا بناء على أدلة محددة سلفا من قبل المشرع، فيحكم القاضي في الدعوى المطروحة أمامه عن توافرت الشرائط القانونية في الدليل المطروح في الدعوى وفي ذلك تقييد للسلطة التقديرية، حيث يشترط في الدليل أن يكون متعلقاً بالواقعة محل الدعوى وله أهمية تفوق بوضوح تأثيره الضار على الدعوى وقد استبعد المشرع بعض الأدلة على الرغم من توافر الشروط القانونية فيها كالشهادة النقلية أو السمعية، ولكون هذا الوضع يثير مشكلات في الإثبات لبعض المسائل أمام القضاء أقر المشرع العديد من الاستثناءات على القاعدة السابقة لإضفاء بعض المرونة عليها نتيجة لتوسعها مع مرور الأيام.

هذا النظام يقلل من أهمية الدليل المستمد من الحاسب كدليل إثبات في المواد الجنائية باعتبار أن الإشارات الإلكترونية والنبضات الممغنطة التي تعتمد عليها الحاسبات في تشغيلها ليست مرئية للعين البشرية الأمر الذي لا يتأتى معه للمحلفين أو للقاضي وضع أيديهم على الدليل الأصلي (أولي لا ثانوي). قام المشرع الإنجليزي نتيجة ذلك بقبول الإثبات بالمحررات شرط أن يكون للمحرر سجل أو جزء من سجل يعده شخص بمقتضى واجب يقع على عاتقه، وألا يكون مقدم المعلومات ممكناً وجوده أو تتبعه.

ثانيا: نظام حرية الإثبات أو نظام الاقتناع الذاتي للقاضي: هو من أكثر الأنظمة شيوعا في التشريعات الإجرائية ويقتضي عدم تحديد أدلة سلفا بعينها التي يجب أن يستند إليها القاضي

---

(169) هلالي عبد اللاه أحمد –حجية المخرجات الكمبيوترية في المواد الجنائية –دراسة مقارنة –أسيوط– 1999م، ص12.

سلفا بحكمه وإنما يكون متمتعا بسلطة تقديرية واسعة سواء من حيث قبول الادلة ذاتها وعددها أما من حيث تقديره الشخصي لقيمة كل منها كل ذلك تبعا لما يطمئن إليه.

ويستند هذا النظام على عدة مبررات:

1. الإثبات في المسائل الجنائية لا ينصب إلا على وقائع مادية أو نفسية خاصة بالواقعة الإجرامية.
2. ولأن الإثبات ينصرف إلى وقائع إجرامية يعمد الجناة لإزالة آثار جرمهم الأمر الذي يحتم تخويل القضاة كافة الوسائل المتاحة والممكنة لتقصي الحقيقة.

ولا يعني الأخذ بهذا النظام تحكم القاضي واستبداده كون التشريعات الإجرائية تضع ضوابط وقواعد تكفل تجنب استبداد القاضي، وفي الدول التي تأخذ تشريعاتها بهذا النظام قرر المشرع المصري أربعة قيود تحد من حرية القاضي(170):

1. في إثبات المسائل غير الجنائية تتبع المحاكم الجنائية طرق الإثبات المقررة في القانون الخاص بتلك المسائل.
2. والأدلة الخاصة بإثبات جريمة الزنا القبض حال التلبس بالفعل أو الاعتراف أو وجود مكاتيب...
3. بأن يكون الحكم مبنيا على أدلة صحيحة.
4. ضرورة أن يكون اقتناع القاضي يقينيا.

في هذا النظام لا يوجد ما يحول دون قبول مخرجات الحاسب الآلي كأدلة أمام القضاء الجنائي من شأنها أن تسهم في إثبات الدعوى المنظورة أمامه.

ثالثا: نظام الإثبات المختلط: يحتل موقعاً وسطاً بين حرية الإثبات والإثبات المقيد في محاولة لجمع مزاياهما وتلافي عيوبهما، حيث يقوم النظام على تحديد المشرع سلفا لأدلة الإثبات التي يجوز للقاضي الاستناد إليها عند إصداره لحكمه في الدعوى التي ينظرها مع منحه الحق

(170) فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت –لبنان، 2003، ص392.

بتقييم كل دليل على حدة وتقرير كفايته للحكم بالإدانة حيث لا يقوم المشرع بتحديد قيمته ويترك التقدير للقاضي وسلطته التقديرية(171).

وقد أورد الفقه العربي تعريفات متعددة منها أنه: الإطلاع على محل له حرمة للبحث عما يفيد التحقيق، ويعرّف بأنه: إجراء من إجراءات التحقيق، أو أنه: تقوم به سلطة حددها القانون، يتم بالبحث في مستودع السر عن أدلة الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة ويتمثل مستودع السر في شخص المتهم أو في المكان الذي يعمل به أو يقيم فيه، وهو إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة، أما الفقه الغربي، فيعرف الفقه الفرنسي التفتيش بأنه البحث الدقيق لكل عناصر الأدلة التي يمكن استخدامها في الدعوى الجنائية والتي تجري على مسكن المتهم(172).

أما تعريف التحقيق الفني في نظم الحاسوب والإنترنت: البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه، أو الإطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الإنترنت، للاستدلال بها على صدق نسبة الفعل إلى شخص معين أو كذبه(173).

خصائص التحقيق الفني في نظم الحاسوب والإنترنت المستمدة من التعريف والتي تميزه عن غيره من إجراءات التحقيق هي(174):

---

(171) فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت –لبنان، 2003، ص393.

(172) علي طوالبة، رسالة دكتوراه، التفتيش الجنائي على نظم الحاسوب والانترنت– دراسة مقارنة –جامعة عمان العربية للدراسات العليا –2003م.

(173) هلالي عبد اللاه أحمد –حجية المخرجات الكمبيوترية في المواد الجنائية –دراسة مقارنة –أسيوط– 1999م، ص22.

(174) علي طوالبه –التفتيش الجنائي على نظم الحاسوب والانترنت – المرجع السابق.

1. يحوي في مضمونهِ على قدر من الجبر والإكراه حيث أنه تعرض قانوني لحرية المتهم الشخصية أو لحرمة أسراره الموجودة على جهاز الحاسوب خاصته أو على برامج خاصة به أو على بريده الإلكتروني عبر شبكة الإنترنت.
2. إن التفتيش يُعد قيداً على حرمة أو حصانة الشخص الذاتية، ويعتبر قيداً على حرمة أسراره الشخصية، أي فيه مساس بحق السر.
3. وسيلة للبحث عن الأدلة المادية والمعنوية للجريمة وضبطها، والتي تفيد في كشف الحقيقة.

المطلب الثاني

تحديد هوية أعضاء الفريق القائم بالتحقيق والضبط

تعتمد جرائم الحاسب الآلي على تقنية المعلومات ووسائل التكنولوجيا مما أظهر تطوراً في ارتكاب الجريمة وطبيعة الدليل وطريقة كشفه وضبطه، مما يتطلب من الجهة المختصة تزويد الشرطة بالمعارف الضرورية لمعالجة تلك الجرائم[175]، فرجال الشرطة قد تكون لديهم خبرة واسعة في التحقيق ولكنهم يفتقدون للمعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم[176]، أنشأت الأردن سنة 1997 إدارة المختبرات والأدلة الجرمية واستحدثت فيها قسم الحاسب الآلي للقيام بهذه المهمة وعلى الرغم من ذلك لا يزال النقص في الخبرة في هذا المجال موجودا ويشكل عائقاً أمام التحقيق والإثبات في جرائم الحاسب الآلي.

إن العمل في التحقيق في قضايا نظم المعلومات أكبر من أن يتولاه شخص واحد بمفرده، حتى لو كانت المضبوطات هي مجرد حاسب شخصي واحد فيفضل أن يتعاون أكثر من شخص في إنجاز مهمة التحقيق والعثور على الأدلة، ومن الضروري أن يكون لدى فريق التحقيق حاسب

([175]) مناعسة واخرون – جرائم الحاسب الآلي والإنترنت – ط1 – دار وائل – عمان – 2001م، ص291.

([176]) حسن طاهر داود –جرائم نظم المعلومات –ط1 –أكاديمية نايف العربية للعلوم الأمنية –الرياض – 2000م، ص222.

محمول مثبت به بطاقة شبكة ليتمكنوا من أخذ نسخة احتياطية من محتويات الأجهزة التي قد يجدونها في مسرح الجريمة[177].

ويجب ان تتوافر فيمن يقوم بتنظيم الضبط والمحاضر التمتع بصفة الضابطة العدلية بموجب نص عام أو نص خاص وكذلك أن يكون مختصا في تنظيم الضبط في الواقعة المعينة وهو ما يسمى بالصفة والاختصاص، ويجب عليه قبل مباشرة عمله أن يحلف اليمين ولمرة واحدة حتى لو انتقل إلى مكان آخر.

في الجريمة التقليدية عند وقوعها الضابطة العدلية تقوم بالتحقيق ممثلة بالنيابة العامة، وقاضي الصلح في الأماكن التي لا يوجد فيها مدعي عام يقوم بممارسة عمله بصفة مدعي عام[178]. وفي المادة 9 عدد المشرع الأردني بعد التعديل الضابطة العدلية والمساعدون[179]، وأضاف آخرون يحالو إلى المادة، وفي حال التبليغ عن الجريمة سواء عن

([177]) حسن طاهر داود –جرائم نظم المعلومات –ط1 –أكاديمية نايف العربية للعلوم الأمنية –الرياض – 2000م، ص223.

([178]) نصت المادة 24 من قانون أصول المحاكمات الجزائية على:"

1. لا يجوز لقاض أن يحكم بالدعوى التي تولى وظيفة النيابة العامة فيها.
2. وإنما يجوز لقاضي صلح النظر في دعوى قام بالتحقيق فيها كمدعي عام، بشرط أن لا يكون قد اتخذ قرار ظن فيها".

([179]) نصت المادة 9 من قانون أصول المحاكمات الجزائية على"

1. يساعد المدعي العام في إجراء وظائف الضابطة العدلية:
- الحكام الاداريون.
- مدير الامن العام.
- مديرو الشرطة.
- رؤساء المراكز الأمنية.
- ضبلط وأفراد الشرطة.
- الموظفون المكلفون بالتحري والمباحث الجنائية.
- المخاتير.
- رؤساء المراكب البحرية والجوية.

وجميع الموظفين اللذين خولوا صلاحيات الضابطة العدلية بموجب هذا القانون والقوانين والأنظمة ذات العلاقة.

طريق تقديم شخص لشكوى تحريرية أو عن طريق الاخبارات والإبلاغات فيقوم المدعي العام بتحريك دعوى الحق العام، أما الجرائم المتعلقة على حق شخصي وضع المشرع قيود ترد على تحريك المدعي العام للدعوى وهذه القيود في دعوى الشرف مثلا التي تحرك بناء على شكوى أو طلب أو إذن.

وفي جرائم الحاسوب تكون النيابة العامة هي المسئولة عن تحريك دعوى من قبل المدعي العام بشكوى الحق العام وإن وجد متضرر فبناءاً على حق شخصي، وهناك جهة متخصصة في جرائم الحاسوب من حيث الاختصاص النوعي فالإجراءات والتحقيق في هذه الجرائم يحتاج إلى جهة مختصة حيث النيابة العامة والشرطة لا تكفي للتحقيق في القضايا المعلوماتية كونها تتطلب تقنيين وخبراء مختصين، وهنا تظهر الحاجة لتزويد الضابطة العدلية بالمعرفة اللازمة عن طريق الدورات التدريبية للضابطة العدلية والشرطة والقضاة والمدعين العامين. وللمدعي العام أن يقوم بالإنابات حسب المادة 92 من قانون أصول المحاكمات الجزائية[180].

صفات المحقق:

1. الالمام الفني والتعرفي للتعامل مع هذا النوع من الجرائم: المشكلة الاساسية التي تواجه المحققين في جرائم نظم المعلومات هي خلفية المحقق نفسه حيث تكون لديه المعرفة التقنية ولكنه غير مدرب على تفهم دوافع الجريمة وجمع الادلة لتقديم المتهم إلى المحاكمة، فيجب تدريبه على تقنيات الحاسب وأساليب التحقيق ومواد القانون والجمع بين خلفية متخصص

---

2. يقوم كل من الموظفين المذكورين بوظائف الضابطة العدلية في نطاق الصلاحيات المعطاة لهم في هذا القانون والقوانين الخاصة بهم.

(180) نصت المادة92 من قانون أصول المحاكمات الجزائية على:"

1. يجوز للمدعي العام أن ينيب أحد قضاة الصلح في منطقته أو مدعي عام آخر لإجراء معاملة من معاملات التحقيق في الامكنة التابعة للقاضي المستناب وله أن ينيب أحد موظفي الضابطة العدلية لأية معاملة تحقيقية عدا استجواب المشتكى عليه.
2. يتولى المستناب من قضاة الصلح أو موظفي الضابطة العدلية وظائف المدعي العام في الأمور المعينة في الاستنابة".

الحاسب والمحقق مهم جدا. مع اتباع القاعدتين الاساسيتين في التحقيق وهما: ضرورة عدم إدخال أي تعديل على الوضع الذي تجد عليه الحاسب، وعدم السماح للمتهم باستخدام الحاسب موضوع الجريمة أو أي حاسب آخر متصل بالشبكة[181].

2. يجب أن تتوفر لدى المحقق الرئيسي خبرة واسعة في التحقيق في القضايا المعقدة فهو يدير العمل ويوجه باقي المحققين وكون قضايا نظم المعلومات تكون أكبر من أن يتولاها شخص واحد يتعاون بها عدة أشخاص لانجاز مهمة التحقيق. فهناك فريق استجواب وفريق تصوير ورسم وفرق تفتيش، وفرق مداهمة، فريق جمع الأدلة.

ويؤدي القضاء دورا مهماً في مكافحة الجرائم التي تعتدي على المصالح الاقتصادية والاجتماعية محل الحماية القانونية ويتطلب ذلك قاضياً يعرف دوره جيدا متفهما للتقدم التقني وما ينتج عنه من وسائل إجرامية يغلب عليها الطابع التقني، والقاضي الجنائي بما له من سلطة يدرك الحاجة إلى الإلمام ببعض المعرفة الفنية بالحاسبات وأنظمتها. وتواجه جرائم الحاسب الآلي صعوبة في تعيين أدلتها بواسطة القاضي الجنائي في ضوء أنظمة الإثبات السائدة زيادة على أن التكييف القانوني للأفعال المستحدثة بواسطة التشريعات التجريمية الحديثة والخاصة بهذه الجرائم تختلف عن نظيرتها في المجال التقليدي.

يقضي القاضي الجنائي في الدعوى التي ينظرها بموجب قناعة يستمدها من أدلة الدعوى المطروحة عليه عند نظره إياها وترتبط قناعة القاضي ارتباطا وثيقا بنظرية الإثبات الجنائي وهي "إقامة الدليل أو الوقوف على حقيقة الوقائع التي تترتب عليها أو تنفيها آثار شرعية أو نظامية"[182]، وإنما الدليل في مجال الإجراءات الجنائية هو "كل إجراء معترف به قانونا لإقناع القاضي بحقيقة الواقعة".

([181]) حسن طاهر داوود، جرائم نظم المعلومات، اكاديمية نايف العربية للعلوم الأمنية، ط1، الرياض، 2000، ص222.

([182]) فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت –لبنان، 2003، ص385.

المطلب الثالث

تقرير إمكانية إتلاف المتهم للدليل أو التسبب بأضرار أكبر

إن مكافحة جرائم الكمبيوتر والانترنت أبرزت العديد من التحديات والمشكلات التي تتعلق بالدليل الالكتروني حيث أن هذه الجرائم لا تترك أثرا في مسرح الجريمة كما أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة[183]. فمن السهل محو الدليل أو تدميره وذلك بالضغط على زر لوحة التحكم ومن ثم صعوبة تحديد الفاعل وكشفه، ويعمل الجاني على إعاقة الوصول للدليل بوسائل حماية مختلفة كاستخدام كلمة سر كحماية لمنع الدخول للأنظمة، فضلاً عن إضافة لضخامة تكاليف جمع الأدلة[184].

وأن التفتيش على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات قد يتجاوز النظام المشتبه به إلى أنظمة مرتبطة مما يخلق تحديات كبيرة أولها مدى قانونية هذا الاجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لاصحاب النظم التي يمتد إليها التفتيش.

وأن الضبط لا يتوقف على تحريز جهاز الكمبيوتر بل يمتد لضبط المكونات المادية لمختلف أجزاء النظام التي تزداد يوما بعد يوم، والضبط ينصب على المعطيات والبرامج والبيانات المخزنة في النظام أو النظم المرتبطة بالنظام محل الاشتباه ذات الطبيعة المعنوية والمعرضة بسهولة للتغيير والإتلاف[185].

([183]) يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الامن العربي2002–تنظيم المركز العربي للدراسات والبحوث الجنائية– أبو ظبي10–2002/2/12.

([184]) أنظر: مناعسة واخرون – جرائم الحاسب الآلي والإنترنت – ط1 – دار وائل – عمان – 2001م، ص289 وما بعدها.

([185]) يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الامن العربي2002–تنظيم المركز العربي للدراسات والبحوث الجنائية– أبو ظبي10–2002/2/12.

وأدلة الإدانة ذات نوعية مختلفة فهي معنوية الطبيعة كسجلات الكمبيوتر ومعلومات الدخول والاشتراك والنفاذ والبرمجيات التي تثير مشكلات حجّة أمام القضاء من حيث مدى قبولها وحجيتها والمعايير المتطلبة في قواعد الاثبات. وأن اختصاص القضاء بنظر جرائم الكمبيوتر والقانون المتعين تطبيقه ليست واضحة ومرور هذه الأفعال عبر الحدود يبرز أهمية قواعد الاختصاص والقانون الواجب التطبيق[186].

وما تقدم يشير إلى الحاجة إلى سرعة الكشف خشية ضياع الدليل، وكذلك خصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم، وكذلك قانونية وحجية أدلة جرائم الكمبيوتر والانترنت، ومشكلات الاختصاص القضائي والقانون الواجب التطبيق، والحاجة إلى تعاون دولي شامل في حقل امتداد إجراءات التحقيق والملاحقة خارج الحدود، وهذه المشكلات كانت ولا تزال محل اهتمام الصعيدين الوطني والدولي.

تتم هذه الجرائم في بيئة افتراضية، بأفعال على شكل نبضات الكترونية غير مرئية لا تترك أثرا حيث يسهل محو الدليل وتدميره، وكما يتم إعاقة الوصول إلى الدليل بوسائل الحماية المختلفة بوضع منظومات حماية تمنع الدخول والنسخ بكلمة السر أو بإتلاف الدليل عند محاولة الدخول غير المصرح به، زيادة على ضخامة تكاليف جمع الأدلة.

وأن قلة الخبرة وضعف الثقافة بتقنية المعلومات تشكل أكبر المشاكل فضلاً عن مشكلة الاختصاص كونها جرائم عابرة للدول وغالبية الدول تتبنى فكرة الاقليمية لتحديد الاختصاص مما يصعب معه متابعة الجرائم بين الدول.

([186]) يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الامن العربي2002–تنظيم المركز العربي للدراسات والبحوث الجنائية– أبو ظبي10–2002/2/12.

المبحث الثالث

الإثبات الجنائي في بيئة الحاسوب والإنترنت

يقوم القضاء بدور هاما في مواجهة حالات التعدي الماس بمصالح المجتمع وأفراده وذلك من خلال تطبيق القوانين وتفسيرها بما يتفق والغاية من سنها والمصالح التي تحميها.

إن التعاون الدولي مهم عند التعامل مع جرائم الانترنت كونه سيطور أساليب متشابهة لتحقيق قانون جنائي وإجرائي لحماية شبكات المعلومات الدولية خاصة أن هذه الجرائم هي عابرة للقارات ولا حدود لها، وفي المقابل فإن عدم التعاون الدولي سيؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول مما سيعطي الفرصة للمجرمين من الإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية[187].

المشكلة الرئيسية في مجال إثبات جرائم الحاسوب والانترنت أنه يصعب اكتشافها وإذا اكتشفت يصعب ملاحقتها وضبطها، ومرتكبوها يتموسون بالدهاء والذكاء والسرعة الفائقة في ارتكاب هذه النوعية من الجرائم وأن الأدلة التقليدية غير ملائمة لأثبات تلك الجرائم، وفي هذه الجرائم اصطدم أجهزة الأمن بتكنيك معلوماتي غير مسبوق (سواء كمحل للجريمة أو كوسيلة مستحدثة لارتكابها) وهو قدرة المجرمين على استحداث وسائل مبتكرة على الدوام إذ يستطيع الجاني أن يرتكب جريمته دون أن يترك وراءه أي أثر خارجي ملموس وإذا كان ثمة دليل على الإدانة فيستطيع الجاني تدميره في ثوان معدودة خاصة وأن المجرم المعلوماتي يتميز بالذكاء وبمهارة تقنية عالية ومعارف فنية في مجال المعلوماتية وأنظمة وبرامج الحاسبات الآلية، وهو على دراية بالأسلوب المستخدم في التشغيل واللغة المستخدمة في تخزين المعلومات وكيفية استدعائها، بل قد يكون من المتخصصين في مجال تقنية المعلومات[188].

([187]) عبد الرحمن عبد العزيز الشنيفي، حرب المعلومات – الحرب القادمة، ص113.

([188]) محمد محيي الدين عوضين، مشكلات السياسية الجنائية المعاصرة في جرائم نظم المعلومات، ص476.

ومما يزيد من صعوبة إثبات الجريمة ثم اكتشافها الرغبة في استقرار حركة التعامل محاولة اخفاء اسلوب ارتكاب الجريمة حتى لا يتم تقليدها من جانب الآخرين يدفع المجني عليه إلى الإحجام عن مساعدة السلطات المختصة في إثبات الجريمة أو في الكشف عنها وحتى في حالة الإبلاغ فإن المجني عليه لا يتعاون مع جهات التحقيق خوفا مما يترتب على ذلك من دعاية مضادة وضياع لثقة المساهمين[189].

وتعود أسباب صعوبة إثبات الحاسب الآلي إلى خمسة أمور وهي:

1. أنها جريمة لا تترك أثراً لها بعد ارتكابها.
2. صعوبة الاحتفاظ الفني بآثارها إن وجدت.
3. أنها تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها.
4. أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.
5. أنها تعتمد على قمة الذكاء في ارتكابها[190].

المطلب الأول

الشروط الواجب توافرها في الدليل الإلكتروني

يتكون الحاسب الآلي من قسم مادي يشمل وحدات الإخراج والإدخال والذاكرة الرئيسية ووحدات المعالجة المركزية، وقسم معنوي يشمل البرامج إضافة إلى البيانات والملفات المختلفة وكلاهما يخضع للتفتيش.ويقسم التفتيش إلى تفتيش مادي وتفتيش قانوني حيث يمثل التفتيش المادي كل صور التفتيش التي لم يرد نص لها في قانون أصول المحاكمات الجزائية، أما التفتيش القانوني فهو ما ورد في قانون أصول المحاكمات الجزائية، ويقسم التفتيش القانوني بدوره إلى تفتيش شخصي وتفتيش منازل. ينصب التفتيش على مستودع السر الذي يشمل الأماكن المسكونة والمعدة للسكن وملحقاتها والاشخاص.

([189]) ذكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، ص477.

([190]) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com

التفتيش الشخصي: **ونعني به تفتيش الشخص نفسه وتفتيش ملابسه بناء على مذكرة صادرة بتفتيشه ويشمل كذلك المكان الذي يتواجد فيه الشخص، وتفتش المرأة من امرأة وفق المادة 86 من قانون أصول المحاكمات الجزائية[191]. ونص ذات القانون على تفتيش الاشخاص من الضابطة العدلية أو المدعي العام وهو التفتيش الذي يعتبر إجراء من إجراءات التحقيق وليس التفايش الاداري أو الوقائي أو الامني أو الضروري يهدف إلى ضبط أدلة الجريمة[192]. وأجازت المادة 97 من القانون نفسه لموظفي الضابطة العدلية تفتيش الاشخاص الموجودين في المنزل في حال الاشتباه بهم بأنهم يخفون مواداً يجري البحث والتحري عنها وتفيد في كشف الحقيقة.**

تفتيش المنازل: **حسب نص المادة 2 من قانون العقوبات يعرف المسكن: " وتعني عبارة بيت السكن المحل المخصص للسكنى أو أي قسم من بناية اتخذه المالك أو الساكن إذ ذاك مسكنا له ولعائلته وضيوفه وخدمه أو لأي منهم وإن لم يكن مسكونا بالفعل وقت ارتكاب الجريمة وتشمل أيضا توابعه وملحقاته التي يضمها معه سور واحد.**

وبناء على ما تقدم إذا كان الحاسوب داخل المنزل فيحتاج لمذكرة تفتيش المنازل أما إذا كان محمولا من قبل الشخص خارج المنزل فيحتاج لمذكرة تفتيش شخصي، وكذلك في حال وجد الجهاز في عيادة طبيب أو مكتب محامي بصفته الشخصية أو سيارة فيحتاج لمذكرة تفتيش أشخاص.

([191]) نصت المادة 86 من قانون أصول المحاكمات الجزائية الاردني على:"

1. للمدعي العام أن يفتش المشتكى عليه وله أن يفتش غيره إذا اتضح من إمارات قوية أنه يخفي أشياء تفيد في كشف الحقيقة.
2. وإذا كان المفتش أنثى فيجب أن يكون التفتيش بمعرفة أنثى تنتدب لذلك."

([192]) محمد صبحي نجم، الوجيز في قانون أصول المحاكمات الجزائية، دار الثقافة- الاردن، ط1، 2006، ص263.

يعد التفتيش من إجراءات التحقيق لا يملكه إلا سلطة التحقيق وهو ممنوع على رجال الضابطة العدلية إلا في حالات الجرائم المشهودة[193]. أما المادة 33 من ذات القانون خولت رئيس الضابطة العدلية ما يلي: "إذا تبين من ماهية الجريمة أن الأوراق والأشياء الموجودة لدى المشتكى عليه يمكن أن تكون مدار استدلال على ارتكابة الجريمة فللمدعي العام او من ينيبه أن ينتقل حالا إلى مسكن المشتكى عليه للتفتيش عن الاشياء التي يراعى مؤدية إلى إظهار الحقيقة".

تفتيش كيانات الحاسوب المادية والمعنوية وضبطها:

الجانب المادي للحاسب الآلي:

يمكن إخضاع المكونات المادية للحاسب الآلي لنظرية التفتيش ومكان وجود هذه المكونات يبين طبيعة إجراءات التفتيش الواجب اتباعها، فوقوع جريمة حاسب آلي يعطي صاحب الاختصاص صلاحية القيام بالتفتيش في كل مكان سواء أكان مسكناً أو محلاً عاماً أو شخصياً أو غيره يمكن الحصول منه على أدلة تثبت وقوع الجريمة ونسبتها لفاعل.

الجانب المعنوي للحاسب الآلي

قد تكون المكونات المعنوية للحاسب الآلي من بيانات وبرامج ومعلومات محل لارتكاب جريمة ما أو وسيلة لارتكاب جريمة ما، وبناء عليه يتم إصدار إذن قضائي بتفتيش الحاسب الآلي للبحث عن أدلة.

(193) محمد صبحي نجم، الوجيز في قانون أصول المحاكمات الجزائية، دار الثقافة– الاردن، ط1، 2006، ص258.

في حال تفتيش حاسب آلي منفرد يعامل معاملة المنزل[194]:

1. المالك ملزم بتزويد الجهة المختصة بالتفتيش بكلمة الدخول على أساس اعتبارها مفتاح البيت.
2. للجهة المختصة بالتفتيش التجول داخل محتويات الحاسب الآلي بحثا عن الأدلة بموجب إذن التفتيش.
3. ولها صلاحية ضبط ما يؤيد التهمة أو البراءة، أو أدلة لجريمة أخرى أو أشياء يحضر اقتناؤها.
4. قد تسجل جهة التفتيش أو تنسخ محتويات الحاسب الآلي على ورق ولها استخدام أي نظام ممكن للتفتيش.

تفتيش حاسب آلي مرتبط بأخر موجود داخل أو خارج الدولة[195]:

1. عند تفتيش حاسب متصل مع حواسيب أخرى داخل الدولة تملك جهة التفتيش البحث عن الأدلة الجرمية على طول شبكات الاتصال المحلية وخارج الحيز المكاني المحدد في إذن التفتيش بشرطين:

أ. احتمال وجود أدلة جرمية تساعد في ظهور الحقيقة.

ب. مراعاة ضوابط وشروط التفتيش المقررة قانونا بالنسبة للمكان أو الشخص كتمتعه بالحصانه وغيره...، ذلك برغم أن قانون أصول المحاكمات الجزائية الأردني يصرح بصلاحية ولوج الجهة المختصة للنهاية الطرفية للحاسب الآلي.

(194) اسامة مناعسة واخرون – جرائم الحاسب الآلي والإنترنت – ط1 – دار وائل – عمان – 2001م، ص279.

(195) اسامة مناعسة واخرون – جرائم الحاسب الآلي والإنترنت – ط1 – دار وائل – عمان – 2001م، ص280.

2. عند تفتيش حاسب آلي موجود خارج الدولة لا تملك جهة التفتيش تجاوز حدود الدولة فتصبح إن تجاوزت غير مختصة مكانيا دون صلاحيات للتفتيش وفي ذلك انتهاك لسيادة الدول الأخرى، وذلك على الرغم من إمكانية التعاون الدولي في هذا المجال.

تفتيش شبكات الاتصال الالكترونية:

نصت المادة 88 جزائية على أنه "للمدعي العام أن يضبط لدى مكاتب البريد كافة الخطابات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق كافة البرقيات ويجوز له مراقبة المحادثات الهاتفية متى كان لذلك فائدة في إظهار الحقيقة". وبما أن وسائل الاتصالات الحديثة معتمدة إلى حد كبير على التقنية ذاتها كاعتمادها على خطوط الهاتف مثلا، هذا يساعد على مد صلاحية التنصت والمراقبة للمراسلات الإلكترونية مع الاحتفاظ بالضوابط القانونية وهي أن تكون دعوى الحق العام محركة، وأن تكون الصلاحية مقتصرة حصرا على المدعي العام، وأن يكون للتنصت والمراقبة فائدة في إظهار الحقيقة[196].

ومن الصعوبات المتعلقة بالتفتيش أن جرائم الحاسب الآلي جرائم حديثة، من حيث نوع الدليل المعتمد في الإثبات وصعوبة كشفه وضبطه وحاجته لخبرات معينة، هذه المواصفات أوجدت كثير من المشاكل العملية في التحقيق والاثبات، فجرائم الحاسب الآلي غالبا غير محسوسة لا تترك دلائل مادية.

لا يقدم المجني عليهم شكاوى في جرائم الحاسب الآلي إما لخوفهم على سمعتهم وأعمالهم التجارية أو لغياب النص التجريمي لما وقع عليهم من سلوكيات أو لجهلهم لما حدث من جرائم، فلا تصل القضاة جرائم حاسب آلي بشكل عام فلا يتعاملون مع تقنية معلوماتية تحتاج لخبرة وفن ودراية، وعند توافر المخرجات الكمبيوترية دليلاً يجب على القاضي بحث الظروف والملابسات مع الأخذ بالدليل العلمي للكشف عن الحقيقة بأن تكون درجته قطعية وألا يمس بحقوق وحريات

([196]) اسامة مناعسة واخرون – جرائم الحاسب الآلي والإنترنت – ط1 – دار وائل – عمان – 2001م، ص284.

الافراد إلا بالقدر المسموح به قانونا حينها يمكن البت في مسألة قبول أو عدم قبول ما يتمخض عن الحاسب الآلي من أدلة إثبات[197].

المطلب الثاني

حجية الدليل الإلكتروني

انقسمت الآراء إلى ثلاثة اتجاهات فيما يتعلق بمدى قناعة القاضي وحريته بالأخذ بالأدلة للإثبات:

أولا: اقتناع القاضي وحريته الوجدانية وفي هذا الاتجاه التشريعي كافة وسائل الاثبات متاحة وذلك يستنتج من أي دليل ويسير على هذا الاتجاه التشريع الاردني والمصري والسوري واللبناني فالقاضي الجنائي له حرية.

ثانيا: تحديد وسائل الاثبات فالقاضي الجنائي محدد بوسائل وطرق التعامل مع الدليل وتحديد الشروط الواجب توافرها فيه.

ثالثا: نظام مختلط مطبق في اليابان والتشيلي وبعض دول العالم الثالث وهو يجمع مابين تحديد الدليل والشروط الواجب توافرها فيه بالإضافة إلى قناعة القاضي.

كانت القرائن في ظل التشريعات التي تأخذ بنظام الأدلة القانونية تختلف من حيث قيمتها في الاثبات وكانت لا تكفي وحدها للإدانة بل يجب أن تدعمها أدلة أخرى كي تصلح للإثبات[198]. ولكن عمدت حل مبدأ الاقتناع الشخصي للقاضي الجزائي محل نظام الأدلة القانونية أصبحت جميع الادلة مقبولة في الاثبات[199]. للقاضي الجزائي مطلق الحرية في أن

---

(197) هلالي عبد اللاه أحمد –حجية المخرجات الكمبيوترية في المواد الجنائية –دراسة مقارنة –أسيوط– 1999م، ص47.

(198) أحمد فتحي سرور، الوسيط في الاجراءات الجنائية، المرجع السابق، ص 350.

(199) محمد صبحي نجم، الوجيز في قانون أصول المحاكمات الجزائية، دار الثقافة– الاردن، ط1، 2006، ص357.

يصل إلى الحقيقة من أي دليل قانوني يستمده سواء أكان هذا الدليل شهادة شاهد أو اعتراف متهم أو ضبط أشياء متعلقة بالجريمة أو وثائق خطية أو ملابسات أو قرائن[200].

الشروط والقواعد العامة الواجب توفرها في الدليل المستخلص:

1. **الانسجام مع أحكام القانون، عدم مخالفة القانون أو الدستور حتى يقبل أمام المحكمة كالاستحصال عليه بوسيلة مشروعة.**
2. **إمكانية مناقشته، فالقناعة الوجدانية تتطلب المناقشة للدليل.**
3. **أن يكون غير قابل للشك يقيني، فالشك يفسر لصالح المتهم.**

من المعروف أن الأدلة الفنية المضبوطة في نظم المعلومات لها أهمية كبرى وقد يكون فيه الفصل بين الادانة والبراءة للمتهم، ويجب أن يعتني فريق التفتيش وفريق جمع الأدلة بتخزين هذه الأدلة في بيئة مناسبة حتى لا تفسد.

أما أنواع الأدلة[201] وأين يبحث عنها فريق التفتيش:

1. **أدلة ورقية: مثل مخرجات الطباعة والتقارير والرسوم البيانية.**
2. **أجهزة الحاسبات: وتتضمن معها ملحقات الحاسب من شاشات وغير ذلك.**
3. **الأقراص المرنة والأقراص الصلبة: من أهم الأدلة لاحتوائها على بيانات وكلمات مرور وصور وتقارير وخطط ارتكاب الجريمة وغيرها...**
4. **أشرطة تخزين المعلومات: تستخدم لحفظ النسخ الاحتياطية**
5. **القطع الالكترونية: كأجهزة الارسال يجب فحصها للتأكد من طبيعتها خاصة في قضايا التجسس**

([200]) نصت المادة 147 من قانون أصول محاكمات جزائية على: "تقام البينة في المخالفات والجنح والمخالفات بجميع طرق الاثبات وبحكم القاضي حسب قناعته الشخصية".

([201]) حسن طاهر داوود، جرائم نظم المعلومات، المرجع السابق، ص226.

6. أجهزة المودم: تستخدم في نقل المعلومات ويمتاز بعضها بامكانية ان يعمل كجهاز الرد على رسائل الهاتف، ويجب تسجيل الكابلات المتصلة به عند ضبطه.
7. البرامج: تمثل الأدوات الرئيسية التي يستغلها المجرم في ارتكاب جريمة نظم المعلومات
8. الطابعات والأجهزة الخاصة بتصوير المستندات: وما قد تحتويه من أوراق مطبوعة ومصورة أو ما هو مختزن في ذاكرتها من معلومات.

يمكن اعتبار الادلة الصوتية التي تخزن الكترونيا أدلة اثبات قاطعة وذلك يعتمد على دقة الاجهزة المستخدمة في الكشف عن التلاعب، فإذا كانت هذه الاجهزة دقيقة تكشف التلاعب بواسطة خبير تعد دليل قاطع. فالدليل الالكتروني يمكن استخدامه دليلاً قانونياً قاطعاً عندما ينص المشرع على أن المعلومات الالكترونية هي أدلة في الاثبات والمقصود بذلك في القانون المدني القاضي المدني محدد ولا سلطة له ولا تعتبر قناعة القاضي، أما في الجنائي فيؤخذ في القناعة الوجدانية، والدليل الالكتروني في الجنائي يمكن اعتباره قرينة بسيطة يمكن إثبات عكسها واليمين غير موجود في الجنائي رغم أنه موجود في المدني وللأحكام الجنائية حجية على الاحكام المدنية ولذلك الجنائي يعقل المدني.

الشروط الفقهية الواجب توافرها في التسجيلات الصوتية المسجلة الكترونيا:

1. أن تكون منطوية على اعتداء على حق يحميه القانون.
2. تحديد دقيق للشخصية المسجل صوتها أو البريد الالكتروني الخاص بها.
3. تحديد الحديث المراد التقاطه وفق الجريمة والجريمة المتعلقة بها والجريمة المصرح بها.

الفصل الخامس

الجهود العربية والدولية في مواجهة جرائم الحاسوب والانترنت

بدأ الاهتمام بجرائم الحاسوب وطنيا وإقليميا ودوليا من قبل المؤسسات التشريعية والهيئات والمنظمات في الثمانينات حيث تم صك قوانين حماية استخدام الحاسوب وتجريم بعض الأفعال المعتبرة جرائم حاسوب على المستوى الوطني ووضع عقوبات لها وفي ذلك إقرار بعجز النصوص التقليدية عن الانطباق على هذه الجرائم، ونما كذلك نشاط الهيئات والمؤسسات الدولية والإقليمية والجمعيات القانونية المتخصصة بجرائم الحاسوب.

أدى الانتشار الواسع والمتسارع للإنترنت والكمبيوتر والتطور الهائل في عالم البرمجيات وتزايد الاعتماد على بنوك المعلومات والكمبيوتر في تنظيم نواحي الحياة كافة إلى وصول هذه التقنية العالية إلى أيدي الخير والشر معا حيث استغل البعض معرفتهم بالتقنية العالية لارتكاب الجرائم سواء الواقعة على المعلومات أو التي ترتكب بواسطة المعلوماتية، كما اكتسبت جرائم الإنترنت طابعا دوليا باعتبار بعضها من الجرائم العابرة للحدود ويرجع سر تسميتها بالعالمية إلى مزاولة الأنشطة الإجرامية فيها على مستوى عالمي وعبر الدول والحدود نتيجة للتقدم المذهل في

وسائل الاتصالات والمواصلات ولكنها في حقيقتها تعتبر من الجرائم الداخلية التي يعاقب عليها قانون العقوبات الوطني(202).

أما عن حجم هذه الظاهرة على الصعيد العالمي فقد بات أمر ملاحظتها محسوسا ويتمثل ذلك في الإحصائيات المروعة التي تبين تزايد مخاطرها والخسائر الناجمة عنها حتى باتت تشكل تهديدا للأمن القومي وللاقتصاد الدولي، وتختلف الدول بمدى تأثرها بهذا النمط من الإجرام بحسب اعتمادها على المعلوماتية والتقنية العالية، ولذلك فإن التعاون الدولي في مجال مكافحة جرائم الحاسوب والوقاية منها أمر لا مفر منه لعجز الدول فرادى عن ذلك ولأن أثر هذه الجرائم أيضا لا يقتصر على النطاق الدولي بل يمتد إلى العالمية.

ولكن التعاون الدولي يواجه الكثير من الصعوبات، فالتشريعات التقليدية تقف عائقا أمام التعاون، وكذلك الاختلاف على مضمون الأفعال التي تعد من جرائم حاسوب، وأن التمايز الحضاري والتشريعي بين الدول المختلفة ومدى اعتمادها على التقنية العالية معوقات تقف في وجه التعاون الدولي في مجال توفير الحماية الجنائية اللازمة، ولكن هذه المعوقات لا تنفي ولا تنكر الجهود الدولية المبذولة في هذا المجال.

---

(202) محمود أحمد عبابنة، "جرائم الحاسوب وابعادها الدولية"، دار الثقافة للنشر والتوزيع، عمان، 2005، ص118.

المبحث الأول

الجهود الدولية لمواجهة جرائم الحاسوب والانترنت

مع تزايد الخسائر الناجمة عن جرائم الحاسب الآلي وتزايد حجم الأضرار الناشئة عنها والتي تتخطى في أغلب أحيانها حدود الدول لتطال اعتداءاتها أجهزة حاسب آلي مملوكة إلى الأفراد أو إلى المؤسسات المالية أو إلى الحكومات بات أمر التعاون الدولي لمواجهتها ضرورة حتمية، وأكدت المنظمات العالمية والإقليمية على حق الإنسان في حرمة حياته الخاصة من أخطار الاعتداء على البيانات الشخصية، وفي إطار الجهد الدولي المبذول فإن هناك العديد من الهيئات والمنظمات والمجالس الدولية التي تؤدي دوراً ملحوظا في إبرام الاتفاقيات في محاولة منها لترسيخ وجوب التعاون الدولي لمواجهة جرائم الحاسب الآلي وعلى رأسها هيئة الأمم المتحدة والمجلس الأوروبي وبعض الهيئات الأخرى.

المطلب الأول

جهود الامم المتحدة على النطاق الدولي

تبذل الأمم المتحدة جهودا لا يستهان بها في مجال محاولة التصدي لجرائم الحاسب الآلي وتؤكد على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من اجل التعاون على الحد من انتشارها وتعاظم آثارها.

كلف مؤتمر الأمم المتحدة السابع الذي انعقد في ميلانو في إيطاليا في عام 1985م لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعلومات والاعتداء على الحاسب الآلي فأقرت مجموعة من المقترحات والتوصيات لمكافحة الظواهر الإجرامية المتعلقة بالحاسب الآلي وقد تبنى مؤتمر هافانا الثامن هذه التوصيات بعد أن أدخل عليها بعض التعديلات، ويمكن إجمال توصيات مؤتمر هافانا لعام 1990م في المبادئ التالية[203]:

1. تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسسية.
2. تحسين أمن الحاسب الآلي والتدابير المعنية.

([203]) محمود أحمد عبابنة، "جرائم الحاسوب وأبعادها الدولية"، دار الثقافة، عمان، 2005، ط1، ص152.

3. اعتماد إجراءات تدريب كافية للموظفين والوكالات المسئولة عن منع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلي والتحري والادعاء فيها.
4. تلقين آداب الحاسب الآلي كجزء من مفردات مقررات الاتصالات والمعلومات.
5. اعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم في تلك الجرائم.
6. زيادة التعاون الدولي من أجل مكافحة هذه الجرائم.

وفي المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين برعاية الأمم المتحدة في القاهرة عام 1995 أكدت توصياته على وجوب حماية الإنسان في حياته الخاصة وفي ملكيته الفكرية من تزايد مخاطر التكنولوجيا ووجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الإجراءات المناسبة للحد منها.

وفي العام 2000 عقدت الأمم المتحدة مؤتمرها العاشر لمنع الجريمة ومعاملة المجرمين في بودابست في المجر وأكدت على وجوب العمل الجاد للحد من جرائم الحاسب الآلي المتزايدة والمستحدثة، واتخاذ تدابير للحد من أعمال القرصنة.

وتوجهت جهود منظمة الأمم المتحدة في ميدان حماية الحياة الخاصة في مواجهة التقدم التقني وحماية الأفراد وحرياتهم من خطر التعدي عليها وذلك في المؤتمر الدولي الأول لحقوق الإنسان الخاص بأثر التقدم التكنولوجي على حقوق الإنسان (مؤتمر طهران 1968) والتي تبنت الجمعية العامة توصياته وأبرز ما جاء فيها أن الحاسبات الإلكترونية تمثل أكبر تهديد للحياة الخاصة والحرية الشخصية إذ أنها تعد من أدوات المراقبة وأجهزة التطفل الحديثة، وخاصة إذا تم تخزين البيانات الشخصية على الحاسب الآلي وتحليلها مما يكشف عن أنماط التعامل والعلاقات[204].

المطلب الثاني

دور المنظمة العالمية للملكية الفكرية

([204]) حمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت-الجريمة المعلوماتية، دار الثقافة، عمان الأردن، 2004، ص74.

وقعت في العام 1967م في استوكهولم في السويد اتفاقية المنظمة العالمية للملكية الفكرية (wipo) أصبحت هذه المنظمة إحدى الوكالات المتخصصة التابعة للأمم المتحدة، ومن خلال استعراض بنود الاتفاقية فقد أكد الأعضاء حرصهم على دعم الملكية الفكرية في جميع أنحاء العالم بهدف تشجيع النشاط الابتكاري ورغبة منهم في تطوير ورفع كفاءة إدارة الاتحادات المنشأة في مجالات حماية الملكية الصناعية وحماية المصنفات الأدبية والفنية.

وبعد تزايد الحاجة إلى إيجاد نصوص قانونية خاصة لحماية البرامج شكلت المنظمة العالمية للملكية الفكرية (wipo) مجموعة عمل تضم عدد من الخبراء بهدف حماية برامج الحاسب الآلي، وعبر الاجتماعات المتكررة وآخرها تم في العام 1985 وبالتعاون ما بين الويبو واليونسكو في جنيف ساد الاتجاه لدى أغلب الدول الصناعية ودول العالم الثالث إلى الميل إلى خضوع برامج الحاسب الآلي لقوانين حماية حق المؤلف ومنذ ذلك العام وحتى الآن عدلت معظم الدول تشريعاتها الخاصة بحق المؤلف وزادت برامج الحاسب الآلي إلى المصنفات الأدبية المحمية وفقا للقانون[205].

وإذا كانت المنظمة العالمية للملكية الفكرية قد لعبت دورا بارزا في حماية حق المؤلف ولعل قانون تونس النموذجي لحقوق المؤلف الذي تم اعتماده في العام 1976 لتستعين به الدول النامية هو ثمرة جهود منظمة الويبو إلا أن اتفاقية تريبس التي عهدت مهمة تنفيذها إلى منظمة التجارة العالمية ومنذ العام 1995 تؤدي الدور الرئيسي الأكبر مما أدى إلى تناقص دور المنظمة منذ ذلك العام المذكور لان اتفاقية تريبس تضمنت قواعد تتصل بكافة فروع وأقسام الملكية الفكرية.

وقد أبرمت اتفاقية بين منظمة التجارة العالمية والمنظمة العالمية للملكية الفكرية في عام 1996م من أجل التعاون المشترك في مجال الملكية الفكرية لا سيما ما يتعلق منها بتطبيق نصوص اتفاقية تريبس وقد عقدت فعلا اتفاقية أولى عام 1998 تلتها أخرى عام 2001 وتهدف اتفاقية تريبس في مجملها إلى تعزيز دور الدول المتقدمة واصفاف الدول النامية فهي في مجال

([205]) محمود أحمد عبابنة، المرجع السابق، ص162.

الملكية الفكرية ستؤدي الاتفاقية إلى ارتفاع التكلفة الاقتصادية لحقوق الملكية الفكرية كما تعمل على إبطاء عجلة التقنيات في الدول النامية لا سيما الدول العربية وذلك بتعزيزها لسيطرة مفهوم الربح على المصنفات الأدبية والفكرية بعيدا عن توخي مفاهيم التوزيع العادل في نشر تلك التقنيات، كذلك فرض حصار التكنولوجيا عليها[206].

المطلب الثالث

دور المجلس الاوروبي

يقوم المجلس الأوروبي بدور مهم في محاولة الحد من جرائم الحاسب الآلي من خلال إقراره للعديد من التوصيات الخاصة لحماية البيانات ذات الصبغة الشخصية من سوء الاستخدام وحماية تدفق المعلومات في 1981/1/28 وقعت اتفاقية تتعلق بحماية الأشخاص في مواجهة المعالجة الإلكترونية للبيانات ذات الصبغة الشخصية، وفي 1980/9/17 وقع المجلس الأوروبي والسوق الأوروبية المشتركة معاهدة مجلس أوروبا الخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات وقد بدأ السريان الفعلي لهذه الاتفاقية في 1985/10 ويقتصر نطاق تطبيق هذه الاتفاقية على الأشخاص الطبيعيين وتسري على القطاعين العام والخاص بشأن الملفات المعدة آليا حيث تحظى بإلزامية أحكامها لتحقيق حماية البيانات الشخصية المعالجة آليا فضلا عن ذلك فقد صدر عن مجلس أوروبا العديد من التوصيات لتؤكد على توسيع نطاق الحماية لتشمل قطاعات الأنشطة الخاصة كالبيانات الطبية والبحثية والإحصائية[207].

وتوج المجلس الأوروبي جهوده بإصدار اتفاقية شاملة تتعلق بجرائم الحاسب في 2000/4/25 وجاء في مقدمة تلك الاتفاقية أن الدول الأعضاء وحرصا منها على حماية مجتمعاتها في جرائم الحاسب الآلي يجب عليها وضع التشريعات الملائمة وتعزيز التعاون الدولي سيما مع تزايد معدلات الجرائم المرتبطة بالتقنية من جرائم شبكات الحاسب الآلي والاعتداء على

([206]) وليد الزيدي، "القرصنة على الإنترنت والحاسوب " التشريعات القانونية، دار أسامة للنشر والتوزيع، عمان 2003، ط1، ص121.

([207]) محمد أمين أحمد الشوابكة، "جرائم الحاسوب والإنترنت– الجريمة المعلوماتية، المرجع السابق، ص74.

المعلومات الإلكترونية والتي تستلزم جهود مضنية للبحث عن الأدلة والإثبات نظرا للطبيعة الخاصة التي تتمتع بها هذه الجرائم لان الأدلة فيها تخزن وتنتقل بواسطة الشبكات.

وتكونت الاتفاقية من خمسة فصول الفصل الأول من الاتفاقية كان لضبط المصطلحات وأما الفصل الثاني فخصص للإجراءات التي يجب أن تتخذ على مستوى وطني وأشارت الاتفاقية أن على كل طرف مشترك في هذا الميثاق أن يبني تشريعات رادعة لمنع الاعتداءات على الصعيد الوطني، وفي الفصل الثالث من الاتفاقية الذي خصص للتعاون الدولي تضمنت الاتفاقية مبادئ متعدّدة عامة تلزم الدول الأعضاء بالتعاون لاتخاذ الإجراءات والتشريعات الكفيلة بتحقيق التعاون وتطبيق التشريعات الدولية.

وتعد هذه الاتفاقية وان كانت مسودة أو مشروعاً بمثابة القانون بين الدول الأعضاء التي بموجبها تلتزم الدول الأعضاء في المجلس والموقعون على هذه المسودة، بضرورة العمل على تنفيذ أحكامها والخضوع لها واحترام تنفيذها وتطويع النصوص القانونية بالشكل الذي يضمن عدم التعارض مع أحكامها[208].

وبشأن حماية قواعد البيانات بوصفها نتاجا فكريا يتطلب أن تحميه قوانين الملكية الفكرية فقد أصدر الاتحاد الأوروبي.

بتاريخ 1996/3/11 إرشادا حمل الرقم (96\9\CEE) يتعلق بالحماية القانونية لقواعد البيانات بما في ذلك غير الإلكترونية منها وقد وصف المؤلف الفكري وأدخلها ضمن أحكام القوانين التي تحمي الملكية الفكرية وقد حدد مدة حماية مضمون قاعدة البيانات بهذا الحق الخاص بخمس عشرة سنة تبدأ من تاريخ انتهاء صناعة قاعدة البيانات وكل تعديلاً مهماً أو تغييراً تالياً في المضمون من شأنه أن يمنح القاعدة ذاتها حماية قانونية جديدة.

وبشأن مشروع حول معاهدة تتعلق بركائز المعلومات فهناك غياب اتفاق بارز في هذا الخصوص خلال مؤتمر المنظمة العالمية للملكية الفكرية ويبدو واضحا في إرشاد الاتحاد الأوروبي لا سيما إرشاده لعام 1999 يتجه نحو مناغمة بعض مظاهر حق المؤلف والحقوق

([208]) محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، المرجع السابق، ص164.

المجاورة في مجتمع المعلومات، فهو ينص في المادة الخامسة منه على: "...السماح بالنسخ العابر والقانوني...عندما تكون الغاية الوحيدة منه حسن استخدام العمل من دون أن يكون للنسخ في هذه الحالة أي مدلول اقتصادي مستقل ..." [209].

أما مسألة حقوق المؤلف على شبكة الإنترنت فإن هذه المسألة لم تزل تشكل موضوعا هاما اختلفت بشأنه التشريعات والقوانين الدولية إذ أن هناك اختلافات صريحة في وجهات النظر حول بعض النقاط الرئيسية.

المطلب الرابع

الجهود الدولية الأخرى لمواجهة جرائم الانترنت والكمبيوتر

هناك جهود أخرى تزاد على جهود الأمم المتحدة والمجلس الأوروبي وتتمثل في بعض المحاولات الإقليمية ومحاولات وطنية فردية.

فالجمعية الدولية لقانون العقوبات وعبر المؤتمرات التي عقدتها حيث تناولت مدى التحديات التي تنطوي على إساءة استخدام الحاسب الآلي ومدى الضرر الناجم عن الاعتداءات على نظم المعلومات والتي يجب على القوانين الجنائية تجريمها.

ومن الهيئات الدولية التي تعنى بأمور الملكية الفكرية وجرائم الحاسب الآلي الاتحاد الدولي للملكية الفكرية مقره في واشنطن ويدخل في اهتمامات الاتحاد نشر دراسات وإحصائيات منتظمة تتعلق بحجم خسائر الدول من جراء أعمال القرصنة وخاصة المتعلقة بالبرامج.

ولا يستطيع أحد إنكار الجهود التي يبذلها معهد ستنافورد في مجال القانون الجنائي على المستويين الداخلي والدولي وذلك من خلال الدراسات الجنائية والإحصائية.

وإلى جانب هذه الجهود هناك كثير من المؤتمرات التي عقدت في العام 2000م مثل مؤتمر جرائم الحاسب الآلي الدولية عقد بالنرويج بمدينة أوسلو بمشاركة العديد من الدول المعنية والهيئات والمنظمات الدولية, كما أن هناك مجهودات تبذلها مجموعة الدول الثماني والتي تهتم

---

(209) وليد الزيدي، "القرصنة على الإنترنت والحاسوب" التشريعات القانونية، المرجع السابق، ص125.

فـي مجـال الحمايـة مـن جـرائم الحاسـب الآلـي وذلـك فـي اجتمـاعهم فـي واشـنطن فـي العـام 1997[210].

ومن الجهود المبذولة أيضا على المستوى الإقليمي جهد السوق الأوروبية المشتركة حيث صدر عن البرلمان الأوروبي عدة قرارات منها قرار 1979/4/8 الخاص في حماية الفرد في مواجهة التطور التقني للمعلوماتية، والقرار الصادر في 1979/5/8 متعلق بحقوق الفرد في مواجهة التطورات التقنية في مجال البيانات، وقرار 1982/3/9 الخاص بحماية الفرد في مواجهة التطورات التقنية في مجال معالجة البيانات، وإذا كانت الحماية الأوروبية للبيانات الشخصية لم تتوج إلى الآن حول حماية هذه البيانات في الفضاء الإلكتروني إلا أنه وفي خطوة أولى من نوعها صدر إرشاد أوروبي حمل رقم CE\9\96 بتاريخ 1996/3/11يتعلق بالحماية القانونية لقواعد البيانات وفيه حماية مزدوجة للتركيب والتصميم[211].

ومن الجهود التي أرست مبادئ حماية الخصوصية بشأن البيانات الشخصية تلك المتمثلة بمنظمة التعاون الاقتصادي والتنمية OECD والتي اهتمت بشكل عملي بحماية الخصوصية ونقل وتدفق البيانات الشخصية وهي قواعد إرشادية لا تتمتع أحكامها بصيغة إلزامية من الناحية القانونية وهي مقتصرة على الأشخاص الطبيعيين وتسري أحكامها على كلا القطاعين العام والخاص وتتضمن ثمانية مبادئ عامة تتمثل بـ:

1. حدود التجميع: أي أنه يتعين فرض قيود على تجميع البيانات الشخصية، بحيث تحدد البيانات التي تحصل عليها بطرق وأساليب مشروعة ونزيهة مع توافر العالم والرضا بموضوع البيانات محل التجميع من أولي الشأن.
2. نوعية البيانات: حيث تنص على أن تتعلق البيانات بالغاية والغرض الذي سوف تستخدم من أجله فضلا عن كونها دقيقة وكاملة ومحدثة.

([210]) محمود أحمد عبابنة، جرائم الحاسوب وابعادها الدولية، المرجع السابق، ص175.

([211]) محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت–الجريمة المعلوماتية، المرجع السابق، ص75.

3. تعيين الغرض: بحيث يكون الغرض الذي تستخدم فيه البيانات الشخصية محصورا ومحددا سلفا بحيث يكون الاستخدام اللاحق للبيانات مقيدا بها.
4. حدود الاستخدام: والذي يقتضي الالتزام بعدم إفشاء البيانات الشخصية ونشرها بأفعال متعددة لغير المصرح لهم بذلك أو باستخدامها بشكل مغاير ومختلف للأغراض المخصصة لها إلا بموافقة الشخص المعني أو وفقا لأحكام تشريعية.
5. الوقاية الأمنية: بحيث يتطلب ضرورة اتخاذ تدابير وإجراءات أمنية ملائمة وحازمة في إحاطة البيانات الشخصية.
6. الانفتاح: أن تكون السياسة العامة للتطوير والخطط والتطبيقات معلنة فيما يتعلق بالبيانات ذات الطبيعة الشخصية بحيث يكون متاح للكافة معرفتها.
7. المشاركة الفردية: التي تتطلب حق الأشخاص المعنية في الوصول والتعرف على البيانات التي تخصهم فضلا عن رقابة مدى صحتها.
8. المسائلة والمحاسبة: التي تقتضي مسائلة الأشخاص والجهات المرخص لهم الوصول والاطلاع على البيانات والتعامل معها في حالة تجاوز أي من الإجراءات التي تكفل حماية البيانات ذات الصفة الخاصة[212].

ونرى مما تقدم أن الجهد المبذول الداخلي أو الدولي لحماية الخصوصية في مواجهة نظم المعلومات ركز على استظهار ومواجهة الأخطار التي تمثل اعتداءا على الحياة الخاصة للأفراد وبياناتهم الشخصية المخزنة باستخدام الحواسيب ونظمها وشبكات المعلومات ونرى أن الحاجة ملحة لتظافر المزيد من الجهود على المستوى الداخلي والدولي لفرض الحماية على البيانات الشخصية للأفراد وخصوصياتهم لا سيما في ظهور شبكة الإنترنت والطريق السريع للمعلومات الذي أخذت المعلومة الإلكترونية طريقا فيه من خلال التبادل الإلكتروني للبيانات لذا برزت الدعوة إلى تظافر الجهود لوضع قواعد عامة لحماية البيانات لتسترشد بها الدول في تشريعاتها

([212]) محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت – الجريمة المعلوماتية، المرجع السابق، ص76.

الداخلية لحماية البيانات الشخصية من الانتهاك عبر شبكة الانترنت أو أية وسيلة اتصال يكشف عنها العلم.

المبحث الثاني

الجهود العربية لمواجهة جرائم الحاسوب والانترنت

تُعدُّ الجرائم المعلوماتية صورا إجرامية مستحدثة من الجرائم العابرة للحدود الوطنية في عالم ذابت فيه الفواصل وتلاشت الحدود مما جعل من السهولة ارتكاب الجرائم المعلوماتية ليس فقط على المستوى الوطني بل وعلى المستوى الدولي، مما يتطلب التطرق للصعوبات التي تعترض مكافحة تلك الجرائم إذا تجاوز ارتكابها حدود القطر وهذه الصعوبات يمكن تفصيلها وفقا للآتي:

1. عدم وجود مفهوم عام مشترك بين الدول حتى الآن حول نماذج النشاط المكون للجريمة المعلوماتية.
2. اختلاف مفاهيم الجريمة لاختلاف التقاليد القانونية وفلسفة النظم القانونية المختلفة.
3. ليس هناك مفهوم عام حول تعريف القانون للنشاط الإجرامي المتعلق بهذا النوع من الجرائم.
4. عدم التناسق بين قوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحري والتحقيق في الجرائم المتعلقة بالكمبيوتر.
5. نقص الخبرة لدى الأجهزة الأمنية وجهات الإدعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة إن وجدت وجمع المعلومات والأدلة عنها.
6. تعقد المشاكل القانونية والفنية الخاصة بتنفيذ نظام معلوماتي خارج حدود القطر أو ضبط معلومات مخزنة فيه أو الأمر بتسليمها.
7. عدم وجود معاهدات للتسليم أو للمعاونة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي أو عدم كفايتها إن وجدت لمواجهة المتطلبات الخاصة بالجرائم المعلوماتية وديناميكية وسرعة التحريات فيها[213].

([213]) أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، الناشر المؤلف، رقم الإيداع 2003/18588، ص451.

وتعد القوانين والتشريعات العربية متأخرة في مواكبة المستجدات التشريعية العالمية المتعلقة بجرائم الحاسب الآلي الهادفة إلى حماية المنظومة المعلوماتية من الجريمة الإلكترونية ولا سيما الحواسيب الآلية وشبكة الانترنت وقد يعزى ذلك إلى التأخر التقني في مجال المعلوماتية للدول[214].

إذا كانت مجتمعاتنا العربية لم تتأثر بعد بشكل ملموس بمخاطر هذا النمط المستجد من الإجرام فإن خطر جرائم الكمبيوتر والإنترنت المحتمل في البيئة العربية يمكن أن يكون كبيرا لكون الجاهزية الأدائية والتقنية والتشريعية (استراتيجيات حماية المعلومات) لمواجهتها ليست بالمستوى المطلوب إن لم تكن غائبة تماما.

وفي المقابل فقد أمست جرائم الكمبيوتر والإنترنت من أخطر الجرائم التي تقترف في الدول المتقدمة، تحديدا الأمريكية والأوروبية ولهذا تزايدت خطط مكافحة هذه الجرائم وانصبت الجهود على دراستها المتعمقة وخلق آليات قانونية للحماية من أخطارها وبرز في هذا المجال المنظمات الدولية والإقليمية خاصة المنظمات والهيئات الإقليمية الأوروبية وإدراكا لقصور القوانين الجنائية بما تتضمنه من نصوص التجريم التقليدية كان لابد للعديد من الدول من وضع قوانين وتشريعات خاصة أو العمل على جبهة قوانينها الداخلية لتعديلها من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم وتتم مواجهة هذه الجرائم في ثلاث قطاعات مستقلة (حماية استخدام الكمبيوتر أو ما يعرف أحيانا بجرائم الكمبيوتر ذات المحتوى الاقتصادي، وحماية البيانات المتصلة بالحياة الخاصة (الخصوصية المعلوماتية)، وحماية حق المؤلف على البرامج وقواعد البيانات(الملكية الفكرية للمصنفات الرقمية) وهذا بدوره أضعف إمكان صياغة نظرية عامة للحماية الجنائية لتقنية المعلومات[215].

([214]) وليد الزيدي، القرصنة على الانترنت والحاسوب –التشريعات القانونية، المرجع السابق، ص128.

([215]) تحت عنوان: جرائم الكمبيوتر والإنترنت– إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، المحامي يونس عرب، من خلال موقع :www.google.com

المطلب الأول

القانون الجزائي العربي الموحد

لعل أبرز ما يمكن أن يقال عن الجهود العربية المبذولة من أجل الحماية من جرائم الحاسب الآلي اعتماد مجلس وزراء العدل العرب للقانون الجزائي العربي الموحد قانوناً نموذجياً بموجب القرار رقم229 لسنة 1996م وبالرجوع إلى المذكرة الإيضاحية لهذا القانون وباستعراض الباب السابع الخاص بالجرائم ضد الأشخاص نجد أن هذا القانون قد احتوى على فصل خاص بالاعتداء على حقوق الأشخاص الناتج عن الجذاذات والمعالجات المعلوماتية وذلك في المواد 461–464، حيث أشارت المواد 161–163 على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية، وكيفية جمع المعلومات الاسمية وكيفية الإطلاع عليها.

أما المادة 464 فلقد نصت على عقاب من يقوم بفعل الدخول بطريق الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات، وعرقلة أو إفساد نظام التشغيل عن أداء وظائفه المعتادة، وتغيير المعلومات داخل النظام وتزوير وثائق المعالجة الآلية، وسرقة المعلومات، وتعد هذه المحاولة على الرغم من تواضعها أبرز ما تم على صعيد تعزيز التعاون على مستوى وطننا العربي من الناحية التشريعية[216].

المطلب الثاني

الاتفاقية العربية لحماية حقوق المؤلف

أما الجهود العربية المبذولة في إطار حماية الملكية الفكرية وحق المؤلف خصوصا أبرمت الاتفاقية العربية لحماية حقوق المؤلف والتي أوصى مؤتمر الوزراء المسئولين عن الشؤون الثقافية المنعقد في بغداد 1981م الدول العربية بالمصادقة عليها، وجاء في ديباجة الاتفاقية أن الدول العربية إذ تحذوها الرغبة على حد سواء في حماية حق المؤلفين على المصنفات الأدبية

([216]) محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، المرجع السابق، ص171.

والفنية بطريقة فعالة وموحدة، وتجاوبا مع المادة21 من ميثاق الوحدة الثقافية العربية الصادرة عام 1964م التي حثت الدول العربية على وضع تشريعات لحماية الملكية الأدبية والفنية والعلمية.

وأبرمت المنظمة نفسها (المنظمة العربية للتربية والثقافة والفنون) الاتفاقية العربية لتيسير انتقال الإنتاج الثقافي العربي في عام 1987م، وتعدّ هاتان الاتفاقيتان مثالا واضحاً على جهود الجامعة العربية والمنظمات المتخصصة التابعة لها في مجال تنظيم حقوق المؤلف.

وإن كان هذا يعد جهدا متواضعا – نظرا لما تمثله حماية حق المؤلف بوصفها اتجاهاً واحداً من اتجاهات جرائم الحاسب الآلي– إلا أن هذا له ما يبرره فوضع الدول العربية يختلف عن الدول الغربية المتقدمة التي تعتمد على التكنولوجيا في شتى مناحي الحياة، ولا نزال أقل تأثرا بالجرائم الماسة بالملكية الفكرية كما هو الحال في الغرب(217).

المطلب الثالث

الجهود العربية الأخرى لمواجهة جرائم الانترنت والكمبيوتر

أكدت الجمعية المصرية للقانون الجنائي في مؤتمرها السادس المنعقد في القاهرة من 25–28 أكتوبر 1993م حول جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات على عالمية جرائم الحاسب الآلي ووجوب تكاتف الجهود لمكافحتها لأنها تمثل وجها سلبيا للتقدم الحضاري، ووجوب تعديل نصوص قانون العقوبات التقليدية أو إضافة نصوص جديدة لأن النصوص الحالية لا يحيط معظمها بالأنشطة المراد تجريمها، كما خرج المؤتمر بتوصيات خاصة بأنماط أو طوائف جرائم الحاسب الآلي، وتوصيات بالتعاون الدولي في مجال أنظمة المعلومات وتنفيذ ما تقره من قواعد ووجوب تحقيق التعاون الدولي في مجال مكافحة جرائم الكمبيوتر وذلك في مجال الإنابة القضائية وتسليم المجرمين وتنفيذ الأحكام، كما أوصى المؤتمر بوجوب تدريب رجال الضبطية القضائية والنيابة العامة والقضاة على طرق وكيفية استخدام أجهزة المعلومات وطرق الاستدلال والتحقيق وجمع الأدلة في الجرائم المتعلقة بها.

---

(217) محمود أحمد عبابنة، جرائم الحاسوب وابعادها الدولية، المرجع السابق، ص173.

إلى جانب هذه الجهود هناك جهود أخرى كالمؤتمر الدولي العربي الأول للملكية الفكرية المنعقد في عمان عام 1995م حيث نوقشت فيه حماية الملكية الفكرية والإجراءات المطلوبة من الأقطار العربية لتنفيذ اتفاقية تربس وأثر حماية الملكية الفكرية على مستقبل الاستثمار في الشرق الأوسط.

وفي بيروت عقد مؤتمر عام 1997م وطالب في توصياته بضرورة إنشاء محاكم متخصصة للبت في النزاعات المتعلقة بالحماية وتشجيع التعاون بين الدول العربية، أما المؤتمر العربي الدولي الثاني للملكية الفكرية الذي عقد عام 1998م طالب بضرورة توجيه توصية حول تسهيل نقل التكنولوجيا من الدول الصناعية إلى الدول العربية لحماية الاختراعات ومكافحة القرصنة وتسهيل نقل اختراعات العلماء العرب إلى أوطانهم.

أما بالنسبة لمسألة الحماية القانونية للبيانات الاسمية والحياة الخاصة على شبكة الانترنت فلم تتناوله الدول العربية في تشريعاتها أو قوانينها المعمول بها حاليا، وبقي يسود القانون الدولي اختلاف شديد التباين فيما يتعلق بالتشريعات المتعلقة بحماية المعطيات الشخصية، هذا وقد قامت عدد من الدول النامية على مستوى داخلي بوضع خطط لاستيعاب التجارة الالكترونية إلا أن ذلك لم يحدث سوى القليل من التطور فيما يتعلق بالإصلاحات التشريعية في هذا المجال ويرى مراقبون أنه ما لم تتخذ هذه الدول تدابير تشريعية مناسبة فإنها ستواجه منافسة شديدة على مستوى التجارة الدولية في المستقبل.

ولم تتطرق بعد التشريعات والقوانين العربية لفئة الجرائم الواقعة على الأنظمة المعلوماتية مباشرة ولم تتناولها في تشريعاتها وقوانينها، على الرغم من الحاجة الملحة إليها لكي تقدم سبل الحماية والأمن لمنظومة المعلومات والاتصالات الحديثة وفي مقدمتها شبكة الانترنت[218].

---

(218) وليد الزيدي، القرصنة على الإنترنت والحاسوب، المرجع السابق، ص160.

المبحث الثالث

التشريعات والقوانين الوطنية الأجنبية لمواجهة جرائم الإنترنت

اتجهت كافة الدول المتقدمة تكنولوجيا إلى استحداث نصوص قانونية جديدة تجرم الجرائم الإلكترونية الجديدة على قوانينها التقليدية القديمة وصاغت تلك الدول نصوص قانونية جديدة قادرة على التعامل مع تلك الجرائم الجديدة والمتطورة تكنولوجيا.

فالتعاون الدولي مهم عند التعامل مع جرائم الإنترنت كونه سيطور أساليب متشابهة لتحقيق قانون جنائي وإجرائي لحماية شبكات المعلومات الدولية خاصة أن هذه الجرائم هي عابرة للقارات ولا حدود لها وفي المقابل فإن عدم التعاون الدولي سيؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول مما سيعطي الفرصة للمجرمين من الإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية.

المطلب الأول

السويد

تعدُّ السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والإنترنت حيث صدر قانون البينات السويدي عام 1973 الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي زيادة على شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها[219].

المطلب الثاني

أمريكا

---

(219) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com

وقد قدرت الولايات المتحدة الأمريكية خسائرها من جرائم الحاسب الآلي، مابين ثلاثة وخمسة بلايين دولار سنويا وقدرت المباحث القدرالية في نهاية الثمانينات الميلادية، وبينت دراسة أجراها أحد مكاتب المحاسبة الأمريكية أن 240 شركة أمريكية تضررت من جرائم الغش باستخدام الكمبيوتر، وأظهر المسح الذي أجري عام 2000 أن مئتين وثلاث وسبعين شركة بلغ مجموع خسائرها أكثر من (256.000.000) دولار[220].

تبعت الولايات المتحدة الأمريكية السويد في إصدار قوانين خاصة تجرم الجرائم الإلكترونية حيث شرعت قانون خاص لحماية أنظمة الحاسب الآلي وفي عام 1985م حدد معهد العدالة القومي الأمريكي خمسة أنواع رئيسية للجرائم المعلوماتية وهي:

- جرائم الحاسب الآلي الداخلية.
- جرائم الاستخدام غير المشروع عن بعد.
- جرائم التلاعب بالحاسب الآلي.
- دعم التعاملات الإجرامية.
- سرقة البرامج الجاهزة والمكونات المادية للحاسب.

وفي عام 1986م صدر قانونا آخر يحمل الرقم 1213 عرف كافة المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية ووضعت المتطلبات الضرورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار التشريعات الخاصة بكل منها على حده للتعامل بها مع تلك الجرائم الالكترونية ومنها القانون الخاص بولاية تكساس لجرائم الحاسب الآلي، وقد خولت وزارة العدل الأمريكية في عام 2000م خمس جهات حكومية للتعامل مع جرائم الانترنت والحاسب الآلي منها مكتب التحقيقات الفدرالي[221].

المطلب الثالث

([220]) محمد عبد الله منشاوي، " جرائم الإنترنت من منظور شرعي وقانوني، مكة المكرمة، 2003/11/1 من خلال الموقع mohammed@minshawi.com

([221]) منير الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص187.

بريطانيا

بينت دراسة أجريت في بريطانيا أنه حتى أواخر الثمانينات ارتكبت ما يقرب من 262 جريمة حاسوبية وقد كلفت حوالي اثنين وتسعين مليون جنيه استرليني سنويا.

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرت قانون مكافحة التزوير والتزييف عام1981م والذي شمل في تعاريفه الخاصة بتعريف آداه التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى[222].

المطلب الرابع

كندا

وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت حيث عدلت في عام1985م قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية وجرائم التدمير أو الدخول غير المشروع لأنظمة الحاسب الآلي، ووضح فيه صلاحيات جهات التحقيق كما جاء في قانون المنافسة الذي يخول لمأمور الضبط القضائي متى ما حصل على أمر قضائي حق تفتيش أنظمة الحاسب الآلي والتعامل معها وضبطها.

ويعد تشريع كيوبك عام1994م تشريع شامل للخصوصية وهو مدعوم ومؤيد من نصوص القانون المدني الذي يحمي الخصوصية بشكل عام ويحترم حماية البيانات الشخصية في القطاع الخاص، وقد قدم هذا القانون مشروع حماية شاملة للبيانات في الحقل الخاص ليكون مجموعة متكاملة عند اكتمال فانون خصوصية القطاع العام[223].

المطلب الخامس

فرنسا

([222]) محمد عبد الله منشاوي، جرائم الإنترنت من منظور شرعي وقانوني، المرجع السابق.

([223]) محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت –الجريمة المعلوماتية، ص80.

فرنسا من الدول التي اهتمت بتطوير القوانين الخاصة بها للتوائم مع الجرائم التكنولوجية الحديثة جرائم الانترنت، فقد طورت فرنسا قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت أول قانون خاص بها في عام 1988م الذي زاد على قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لتلك الجرائم كما تم في عام 1994م تعديل قانون العقوبات لديها ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية وقد أوكل هذا القانون إلى النيابة العامة سلطة التحقيق بما في ذلك طلب عمل التحريات وسماع الأقوال والشهود[224].

أصدر المشرع الفرنسي القانون رقم 7 لسنة 1978 الخاص بالمعالجة الالكترونية للبيانات الاسمية والذي اشتهر باسم قانون معالجة المعلومات والحريات وبينت المادة الأولى منه أن معالجة المعلومات يجب أن تكون في خدمة كل مواطن، ووضعت عدة قوانين روعي فيها التطور التكنولوجي في عالم الاتصالات والكمبيوتر ومنها:

- قانون 1980/7/12 والمتعلق بإثبات التصرفات القانونية ذات المعالجة الالكترونية.
- قانون 1982/6/29 الذي أقر فيه مبدأ حرية الاتصال السمعي والبصري.
- قانون 1986/9/30 المعدل بـ 17/ يناير/1989 بشأن الاتصالات السمعية والبصرية والذي حل محل قانون 1982 المشار إليه.
- قانون العقوبات الجديد لعام 1992 والمعمول به منذ عام 1994[225].

المطلب السادس

الصين

([224]) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص189.

([225]) محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت– الجريمة المعلوماتية، المرجع السابق، ص80.

أصدرت الصين مرسوماً في شهر 2\1996م بشأن تنظيم استخدام الانترنت، حيث فرضت على كل مستخدم لبرامج بث المعلومات عبر الشبكة أن يحصل على موافقة مسبقة من وزارة البريد والاتصالات وأنه يحظر عليه بث أي معلومة يكون من شأنها المساس بالنظام العام[226].

المطلب السابع

هولندا

عدلت قوانينها الخاصة بهذه الجرائم محاولة السيطرة عليها ونصت في قوانينها على أنه من حق القاضي أن يصدر أوامره بالتنصت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة وكان التنصت على قدر من الأهمية للكشف عن الجريمة[227].

المطلب الثامن

فنلندا

هي الأخرى قامت بتعديل قوانينها الجنائية لتتسع لتلك الجرائم الإلكترونية الحديثة وطبقا لتلك التعديلات فقد أصبح لمأمور الضبط القضائي الحق في التنصت على المكالمات الخاصة بشبكات الحاسب الآلي.

المطلب التاسع

ألمانيا

يعطي القانون الألماني الحق للقاضي في إصدار أوامره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام[228].

المطلب العاشر

([226]) المرجع السابق، ص81.

([227]) منير محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص189.

([228]) منير محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص190.

اليابان

في اليابان قوانين خاصة بجرائم الحاسب الآلي والانترنت ونصت تلك القوانين على أنه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته، كما أقرت عام 1991م شرعية التنصت على شبكات الحاسب الآلي للبحث عن دليل[229].

المطلب الحادي عشر

المجر

سنت قوانين خاصة بها لتجرم الجرائم الالكترونية وقد نصت تلك القوانين التي سنتها على كيفية التعامل مع مثل هذا النوع من الجرائم وأيضا كيفية التعامل مع المتهمين بارتكاب الجرائم، وهي الإجراءات التي تسهل عمل الجهات المنوط بها مواجهة مثل تلك الجرائم والقبض على المتهمين بارتكابها.

المطلب الثاني عشر

بولندا

سنت قوانين خاصة بها تنص على أن للمتهم بارتكاب الجرائم الحق في عدم طبع أي سجلات خاصة بالحاسب الآلي أو إفشاء كلمات السر المستخدمة أو حتى الأكواد الخاصة بالبرامج وأنها تنص على حقوق أخرى بالنسبة للشهود في تلك الجرائم فهي تعطي الشاهد أيضا الحق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى كان ذلك قد يؤدي إلى إدانته أو إدانة أي من أقاربه بل إن تلك القوانين تذهب إلى مدى أبعد من ذلك فتلك القوانين تنص على أن لا يقابل ذلك أي إجراء قسري قد يتخذ وتكون من نتائجه إدانة المتهم[230].

([229]) محمد عبد الله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، المرجع السابق.

([230]) محمد عبد الله منشاوي، المرجع السابق.

المبحث الرابع

التشريعات والقوانين الوطنية والعربية لمواجهة جرائم الإنترنت

لم تزل التشريعات والقوانين العربية تخطو خطوات خجولة في مواكبة التطورات التشريعية العالمية المتعلقة بجرائم الإنترنت والكمبيوتر، وسنستعرض في هذا المبحث بعض التشريعات والقوانين العربية التي تبين الجهود التي قامت بها تلك الدول لمواجهة جرائم الإنترنت والكمبيوتر.

المطلب الأول

تونس

أفرد المشرع التونسي حماية خاصة للمعطيات الشخصية في مواجهة التطور التقني في المواد من 38–42 من قانون التجارة الإلكترونية لعام 2000 وفرض عقوبات أصلية وعقوبات تكميلية على الأفعال المخالفة لتلك المواد، فتنص المادة 38 على أنه: "لا يمكن لمزود خدمات المصادقة الإلكترونية معالجة المعطيات الشخصية إلا بعد موافقة صاحب الشهادة المعني، وتنص المادة 39 على أنه: "باستثناء موافقة صاحب الشهادة لا يمكن لمزود خدمات المصادقة الإلكترونية أو أحد أعوانه جمع المعلومات الخاصة بصاحب الشهادة إلا ما كان منها ضروريا لإبرام العقد وتحديد محتواه وتنفيذه وإعداد وإصدار الفاتورة لا يمنك استعمال المعطيات المجمعة طبقا للفقرة الأولى من هذا الفصل لغير الغاية المذكورة أعلاه من قبل المزود أو غيره إلا إذا تم إعلام صاحب الشهادة بذلك ولم يعارضه".

وتنص المادة 40 على أن: "يمنع على مستعملي المعطيات الشخصية المجمعة طبقا للفصل 39 من هذا القانون إرسال الوثائق الإلكترونية إلى صاحب الشهادة الذي يرفض صراحة قبولها ويتعين على صاحب الشهادة إعلام الوكالة الوطنية للمصادقة الإلكترونية باعتراضه بواسطة رسالة مضمونه الوصول مع إعلام بالبلوغ، ويعدُّ هذا الإعلام قرينة قاطعة على معرفة كل المزودين والغير لهذا الاعتراض".

أما المادة 41 فتنص على أنه:" يتعين على مزود خدمات المصادقة الإلكترونية قبل كل معالجة للمعلومات الشخصية إعلام صاحب الشهادة بواسطة إشعار خاص بالإجراءات المتبعة من قبله في مجال حماية المعطيات الشخصية"[231].

ويتعين أن تمكن هذه الإجراءات صاحب الشهادة من الاطلاع آليا وبطريقة مبسطة على محتوى المعطيات، وكذلك تنص المادة 42 على: "يمكن لصاحب الشهادة في كل وقت بطلب ممضي بخط اليد أو إلكترونيا النفاذ إلى المعلومات الشخصية المتعلقة بصاحب الشهادة، ويتعين على المزود وضع الإمكانيات اللازمة لتمكين صاحب الشهادة من إرسال مطلبه الممضي لتعديل المعلومات أو مسحها بطريقة إلكترونية".

فقد تنبه المشرع التونسي إلى خطورة بنوك المعلومات والتطور التقني على المعطيات الشخصية مما حذا به إلى فرض نصوص خاصة تكفل الحماية لحرمة الحياة الخاصة من المعالجة الآلية للمعطيات.

المطلب الثاني

لبنان

في مجال قوانين الملكية الفكرية وفيما يتعلق بحقوق المؤلف المعنوية يعاقب قانون الملكية الأدبية والفنية اللبناني رقم 1999/75على الاعتداءات على حقوق المؤلف جزائيا فضلا عن المسائلة المدنية، إذ يتعرض المعتدي لدفع غرامات باهظة ولتعويض عادل عن العطل والضرر المادي والمعنوي الذي يلحق بصاحب الحق.

ونصت المادة 21 منه على ما تشمله حقوق المؤلف المعنوية بأنها الحقوق التالية: "...حق المؤلف في إشهار عمله...الحق بالمطالبة بأن ينسب إليه العمل كمؤلف له وبأن يذكر اسمه على كل نسخة ...والحق في منع أي تحوير أو تطوير أو تعديل أو تغيير في العمل قد

([231]) محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت –الجريمة المعلوماتية، المرجع السابق، ص81، 82.

يسيء إلى شرفه أو سمعته أو شهرته أو مكانته الفنية والأدبية والعلمية، وأخيرا الحق بأن يستعمل اسما مستعارا أو أن يبقي اسمه مغفلا".

المطلب الثالث

الامارات

تعد في طليعة البلدان العربية التي تسعى لمواكبة المستجدات الحديثة في مجال التشريعات والقوانين المتعلقة بالمنظومة المعلوماتية، فهي لم تعالج قانون المؤلف ذي الرقم 40 لسنة 1992 القضايا الخاصة بالقرصنة وسرقة المؤلفات، بل تطبق قانون حماية الملكية الفكرية الصادر عن الدولة عام 1994 الذي يوجه إلى مستخدمي البرامج غير الشرعية عقوبة الغرامة المالية التي تصل إلى 50 ألف درهم إماراتي ومصادرة أجهزة الحاسوب والبرامج بالإضافة لعقوبة الحبس التي قد تصل مدتها إلى ثلاث سنوات، وتعد دولة الإمارات في صدارة القائمة الإقليمية في مكافحة قرصنة البرمجيات في الشرق الأوسط لعام 2000[232].

ويجري العمل من اجل وضع الأطر القانونية للتجارة الإلكترونية ففي 2001 في أسبوع الحكومة الإلكترونية الثالث تم التأكيد على ضرورة وضع صياغة قانونية وتشريعية للإثبات القانوني والتوقيع الإلكتروني وكل ما يتعلق بالتجارة الإلكترونية، ودعت دولة الإمارات لتشكيل مجلس قضائي للتجارة الإلكترونية بدول مجلس التعاون، ولدى مطالعة قانون الإثبات الإماراتي رقم10 لسنة 1992 يتبين أن أدلة الإثبات منها المستندات لا يعتد بها أو تقبل إلا بشروط وقيود معينة تتعارض مع وضع المستندات الإلكترونية والتواقيع الإلكترونية مما يجعل هناك صعوبة في ممارسة التجارة الإلكترونية[233].

المطلب الرابع

مصر

---

(232) وليد الزيدي القرصنة على الانترنت والحاسوب، المرجع السابق، ص130.

(233) نفس المرجع، ص147.

اتجهت التشريعات نحو تعديل قوانين الملكية الفكرية للتناسب مع التطورات التقنية المستحدثة عالميا، بسن قوانين تحمي البرمجيات وحقوق المستهلكين من جرائم الحاسوب الآلي، فقد عملت جمعيات خاصة من أجل تثبيت حماية حقوق الملكية الفكرية في مجال البرمجيات وعلى رأسها "اتحاد منتجي البرامج التجارية" وقد أسفر ذلك عن انخفاض في نسبة القرصنة إلى نحو 19% في عام واحد فوصلت إلى 56% في عام 2001 بعد أن كانت تلك النسبة 75% خلال العام 1999.

وفي مصر تدرس مسألة الدفع الإلكتروني في مجال التجارة الالكترونية من خلال لجان متخصصة في وزارة الاتصالات والمعلومات وذلك من أجل إصدار قوانين منظمة له.

المطلب الخامس

السعودية

على الرغم من حداثة جرائم الحاسب الآلي والانترنت نسبيا إلا أن الدراسة التي أجرتها منظمة (business software alliance) في الشرق الأوسط في حجم خسائر جرائم الحاسب الآلي وصلت إلى ثلاثين مليون دولار أمريكي في المملكة العربية السعودية والامارات العربية المتحدة.

لم تسن السعودية قوانين خاصة بجرائم الإنترنت، إلا أن وضعها يختلف فهي ليست بحاجة لتحديث قوانينها وتشريعاتها كونها تنطلق من الشريعة الإسلامية الكاملة فالمشرع واحد لا ثاني له والتشريع أزلي لا تجديد له، فهو صالح لكل زمان ومكان فقد تركت الشريعة الإسلامية الباب مفتوحا لتجريم الجرائم المستحدثة تحت قواعد فقهية واضحة منها لا ضرر ولا ضرار وتركت لولي الأمر تقرير العقوبات لبعض الجرائم المستحدثة مراعاة لمصلحة المجتمع ويندرج ذلك تحت باب التعازير، وهناك قاعدة سد الذرائع أي: دفع الوسائل التي تؤدي إلى المفاسد والأخذ بالوسائل التي تؤدي إلى المصالح[234].

([234]) محمد عبد الله منشاوي، جرائم الإنترنت من منظور شرعي وقانوني، المرجع السابق.

وقد تم توجيه الشركات الراغبة في إصدار تراخيص جديدة أو تجديد التراخيص القائمة بتقديم ما يثبت التزامها بقوانين حماية الملكية الفكرية في مجال تقنية المعلومات، وكان قد أقر قانون حماية الملكية في الدولة في المرسوم الملكي م/11 لسنة 1989م وقد جرى عليه تعديل بمرسوم ملكي سنة 1992م.

وبعد أن انضمت المملكة للاتفاقية العالمية لحقوق المؤلف التي وقعت في باريس صدرت تعليمات مشددة جديدة بشأن تطبيق حماية حقوق التأليف على المصنفات الأجنبية، والتي تضم برامج الحاسوب وبرامج ألعاب الحاسوب وقد نصت التعليمات على ضرورة الالتزام الفوري بالتوقف الكلي والنهائي عن ممارسة أعمال نسخ البرامج بأي شكل أو حجة، وتوقف المحلات عن بيع وعرض الكتب والمجلات وأشرطة الفيديو المتخصصة لأن هذا النشاط يخص المحلات المرخص لها فقط، والالتزام بمزاولة بيع النسخ الأصلية للبرامج فقط وقد بدأ العمل بالقرار في 13/تموز/1992[235].

المطلب السادس
عُمان

صدر قانون حماية المؤلف رقم 74 لسنة 1996 من أجل تحديث التشريع السابق لكي يواكب التقنيات الحديثة في مجال المعلوماتية ويعمل على حمايتها علما أن السلطنة انضمت إلى المنظمة العالمية للملكية الفكرية عام 1996م كما عقد منتدى الويبو الدولي عن الملكية الفكرية والمعارف التقليدية في مسقط عام 2000م بغية التصدي لمسألة النهوض بالمعارف التقليدية وصونها وحمايتها من خلال الانتفاع بنظام الملكية الفكرية.

المطلب السابع
سوريا

صدر في سوريا القانون رقم 12 لعام 2001 متضمنا "حماية حقوق المبدعين والمفكرين" وفي جميع المجالات ويشمل نطاق الحماية البرمجيات الحاسوبية بما في ذلك وثائق التصميم، وأعطى القانون المبرمجين الحق في نشر البرامج وطرق النشر وتضمن عقوبات الحبس من

([235]) وليد الزيدي، القرصنة على الإنترنت والحاسوب–التشريعات القانونية، المرجع السابق، ص133.

ثلاثة أشهر إلى سنتين وغرامة مادية لا تقل عن 100 ألف ليرة سورية لكل من اعتدى على أي حق من الحقوق المشمولة بالحماية[236].

المطلب الثامن
البحرين

لا توجد قوانين خاصة بجرائم الإنترنت وإن وجد نص قريب من الفعل المرتكب فإن العقوبة المنصوص عليها لا تتلاءم وحجم الأضرار المترتبة على جريمة الإنترنت، وقد أوكل إلى شركة البحرين للاتصالات السلكية واللاسلكية مهمة تقديم خدمة الإنترنت للراغبين في ذلك، كما أنيط بها مسئولية الحد من إساءة استخدام شبكة الإنترنت من قبل مشتركيها[237].

المطلب التاسع
الأردن

قطع الأردن شوطا ليس بالبسيط في محاولته اللحاق بركب التطور التشريعي والمساهمة في توثيق أواصر التعاون الدولي، ويتمثل ذلك في انضمامه إلى اتفاقية باريس لحماية الملكية الصناعية المبرمة عام 1883م التي تنظم الملكية الصناعية والاختراعات والعلامات التجارية والرسوم والنماذج الصناعية والتي عدلت بموجب تعديل ستوكهولم عام 1967م، كذلك انضمامه إلى اتفاقية بيرن لحماية المصنفات الأدبية والفنية المبرمة عام 1886م والتي عدلت بموجب تعديل باريس عام 1971م[238].

أما عن تجربة الأردن في مكافحة جرائم الإنترنت والكمبيوتر فقانون العقوبات كأساس تحدد بموجبه الجرائم التقليدية ومن القواعد الثابتة في قانون العقوبات أن لا جريمة ولا عقوبة إلا بنص قانوني ولا يجوز القياس وهذا يخص الجرائم التي تتم بأسلوب تقليدي عادي غير إلكتروني أما الجرائم المعلوماتية فلا تتوافر لها حتى الآن نصوص قانونية في قانون العقوبات فما قامت به الأردن للإحاطة بهذه الظاهرة الجرمية كان كالآتي:

- إصدار قانون حماية حق المؤلف.

([236]) وليد الزيدي، القرصنة على الإنترنت والحاسوب–التشريعات القانونية، المرجع السابق، ص134.

([237]) محمد عبد الله منشاوي، جرائم الإنترنت من منظور شرعي وقانوني، المرجع السابق.

([238]) محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، المرجع السابق، ص153.

- تحديث القوانين السائدة إلى قوانين جديدة تجرم جرائم الإنترنت.
- الانضمام إلى المعاهدات والاتفاقيات الدولية التي تعمل على تجريم جرائم الإنترنت.
- اسـتحداث قـوانين جديـدة تقـنن الاسـتخدامات الإلكترونيـة مثـل قـانون المعـاملات الإلكترونية
- إنشاء إدارات جديدة بوزارة الاتصالات تكون مسؤولة عن تلك الجرائم.

الخاتمة

إن مسألة التنظيم القانوني للمشاكل التي يثيرها مجتمع المعلومات في مركز الاهتمام بالفعل منذ سنوات، ويتوالى إدخال التعديلات اللازمة في القوانين القائمة لمعالجة هذه الأوضاع الجديدة في الحياة كما يجري إعداد قوانين جديده، ويجري تشكيل استراتيجيات وتوقعات جديدة، ولكن الاهتمام بالجرائم الإلكترونية أقل من اللازم مقارنة بحجم الضرر الذي تسببه هذه الجرائم.

وإذا افترضنا أن الجهود القانونية القائمة كافية لمعالجة الجرائم التي ترتكب بواسطة أدوات المعلومات التكنولوجية فإن هذه الجرائم تحتاج مزيدا من الفحص، فالحماية منها تتطلب وسائل تكنولوجية وتنظيمية تختلف عن تلك الوسائل التي تتطلبها الجرائم التقليدية ولو كانت مشابهة لكونها ترتكب بأدوات أخرى، وبالتوازي مع التنظيم القانوني يجب علينا أن نتوصل أولا لحل القضايا التكنولوجية المتعلقة بالأمن حتى نتمكن من منع هذه الجرائم.

وحيث أننا نعيش في المملكة الأردنية الهاشمية عصر الانفتاح على العالم ونعتمد اعتمادا يكاد يكون كليا على توظيف إمكانيات التقنية في مختلف الأنشطة الحكومية والأهلية ونظرا لشيوع استعمال الحواسيب ، فإن الحاجة تبدو ملحة لتحديث تشريعاتنا الجزائية على نحو يكفل الحماية الجزائية للبيانات والمعلومات المعالجة آلياً على غرار النصوص الجزائية الذي استنها المشرع في الدول المتقدمة تكنولوجياً والتي تناولت بالحماية المعلومات والبيانات الشخصية المتصلة بالحقوق الخاصة وحقوق الملكية الفكرية لبرامج الحاسوب حيث لا جدوى من تضييع الجهد والوقت في تطويع ولي النصوص القانونية في زمن امسك فله استجابة المؤسسة التشريعية للتطور ضرورة رئيسية لتعزيز وجود الدولة وفاعلية النظام القانونية وتعزيزا لمبدأ "الشرعية الجزائية" حيث لا يعترف قانون أصول المحاكمات الجزائية الأردني لمخرجات الحاسب الآلي بصفة المحرر فليس لها حجية في الإثبات في الدعاوى المدنية، وأن الفقه القانوني الأردني يعتبر مخرجات الحاسوب لا تتمتع بحجية الاثبات عند بحث الدعاوى الجزائية، يوجد ذلك هوة واسعة

في الوضع القانوني والقضائي في الاردن بين الثورة المعلوماتية الحاصلة والمفاهيم التقليدية في عقلية القاضي.

ولا يوجد قواعد منظمة للتفتيش عندما يكون الحاسب الآلي متصل بأخر خارج الدولة، ولا توجد إجراءات تؤخذ بحق صاحب النظام إن رفض تقديم المساعدة لجهة التحقيق، فمن الضروري تطوير وسائل الإثبات بما يواكب التطور في وسائل الإجرام المعلوماتي.

إن صعوبة الإثبات الجنائي لا يمكن أن تكون عقبة في سبيل التجريم فالتجريم مسألة موضوعية والإثبات يتعلق بمسائل إجرائية ولا يمكن أن نجعل صعوبة الإثبات في بعض المسائل الجنائية سببا في عدم التجريم.

وبناء على ذلك نوصي مشرعنا الجزائي بوضع تشريع جزائي خاص بحماية نظم المعالجة للبيانات مع ضمان الحق في المعلومات والحق في الحياة الخاصة، التحديد الواضح الدقيق لصور السلوك المراد تجريمها، مع مراعاة الطابع التقني لجرائم الحاسوب، وإيجاد العقوبات الملائمة على نحو يحقق أهداف العقوبة في الردع العام والخاص، وكذلك النص بشكل واضح وصريح على مسؤولية الشخص المعنوي وإفراد عقوبة مالية خاصة له لعدم كفاية العقوبات التي تسمح بفرضها علية وفقا للأحكام العامة في قانون العقوبات .

ومن ناحية أخرى نوصي أيضاً بعقد دورات تدريبية لأفراد الضابطة العدلية والنيابية العامة والقضاء على أعمدة التحقيق في نظم المعالجة الآلية للبيانات أسوة بما يجري علية العمل في الولايات المتحدة الأمريكية بهدف تأهيل كل الأشخاص المعنيين بجرائم الحاسوب والانترنت وذلك لرفع قدراتهم الشخصية ليمكنهم من التعامل مع هذا النوع من الجرائم ذات التقنية العالية للحد من انتشارها واتساع دائرة نطاقها والتقليل من آثارها السلبية على المجتمع واقتصاد الوطني ،يعقد دورات خاصة ترتكز على أساليب التحقيق في جرائم نظم المعالجة الآلية للبيانات على أن يقوم بذلك فرد مؤلف من مختصين في مجالات تدقيق ومراجعة الحاسبات ومعالجة البيانات والتحقيق الجزائي.

المراجع

1. أحمد حسام طه تمام – الجرائم الناشئة عن استخدام الحاسب الآلي – (الحماية الجنائية للحاسب الآلي) – دراسة مقارنة – دار النهضة العربية – القاهرة – 2000م.
2. أسامة أحمد المناعسة وجلال محمد الزعبي وصايل الهواوشة – جرائم الحاسب الآلي والإنترنت – دراسة تحليلية مقارنة – ط1 – دار وائل – عمان – 2001م.
3. أسامة عبدالله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دراسة مقارنة – ط2 – دار النهضة العربية – القاهرة – 1989م.
4. أسامة محمود أبو عباس، رحلة إلى عالم الإنترنت، ط1، شركة النجار للكمبيوتر والإلكترونيات – الأردن – اربد – 1999م.
5. أحمد فتحي سرور، الوسيط في الاجراءات الجنائية، المرجع السابق
6. أحمد فتحى سرور الوسيط في قانون العقوبات القسم الخاص – القاهرة – الطبعة الثالثة ستة 1992.
7. أحمد عبد الكريم سلامة، الانترنت والقانون الدولي الخاص– فراق أم تلاق، القانون والكمبيوتر والانترنت، المجلد الأول، 2004، ط3.
8. انتصار نوري الغريب – أمن الكمبيوتر والقانون – دار الراتب الجامعية – بيروت – 1994م.
9. أيمن عبد الحفيظ عبد الحميد سليمان، "استراتيجية مكافحة جرائم استخدام الحاسب الآلي"، الناشر المؤلف، رقم الإيداع 18588\2003.
10. محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة، عمان– الاردن، ط1، 2004.

11. محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان– الأردن، ط1، 2005.

12. منير محمد الجنبيهي، ممدوح محمد الجنبيهي، "جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها"، دار الفكر الجامعي، 30 شارع سوتير– الأزاريطة– الإسكندرية،ط2، 2005.

13. وليد الزيدي، " القرصنة على الإنترنت والحاسوب" التشريعات القانونية، دار أسامة، عمان – الأردن،ط1، 2003.

14. تحت عنوان "جرائم الكمبيوتر والإنترنت المعنى والخصائص والصور واستراتيجية المواجهة القانونية من خلال موقع: www.arablaw.org.com

15. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه في القانون الجنائي، جامعة عين شمس –كلية الحقوق، سنة 2004.

16. جميل عبد الباقي الصغير – أدلة الإثبات الجنائي والتكنولوجيا الحديثة – (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية) – دراسة مقارنة – دار النهضة العربية – القاهرة – 2001م.

17. جميل عبد الباقي الصغير – الإنترنت والقانون الجنائي – الأحكام الموضوعية للجرائم المتعلقة بالإنترنت – دار النهضة العربية – القاهرة – 2001م.

18. جميل عبد الباقي الصغير – الجوانب الإجرائية المتعلقة بالإنترنت – دار النهضة العربية – القاهرة – 2001م.

19. جميل عبد الباقي الصغير – القانون الجنائي والتكنولوجيا الحديثة – الكتاب الأول – الجرائم الناشئة عن استخدام الحاسب الآلي – ط1 – دار النهضة العربية – القاهرة – 1992م.

20. جميل عبد الباقي الصغير– الانترنت والقانون الجنائي والأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة 2002.

21. زياد عبد الكريم وآخرون – الكمبيوتر وتطبيقاته – دار المستقبل للنشر – عمان – 1990م.
22. سعيد عبد اللطيف حسن – لإثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت – الجرائم الواقعة في مجال تكنولوجيا المعلومات – ط1 – دار النهضة العربية – القاهرة – 1999م.
23. عمر الفاروق الحسيني – المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية – دراسة تحليلية نقدية – ط2 – القاهرة – 1995م.
24. فاروق محمد العامري – الشبكة العالمية للمعلومات – الإنترنت – ط1 – النسر الذهبي للطباعة – القاهرة – 1977م.
25. فاروق حسين – فيروسات الحاسب الآلي والإنترنت – ط1 – دار هلا للنشر – 1991م.
26. فراس محمد العزة وآخرون، مهارات الحاسوب– الحاسوب والبرمجيات الجاهزة، دار اليازوري العلمية للنشر والتوزيع ، عمان، ط1، 2003، ص13.
27. عبد الفتاح بيومي حجازي – النظام القانوني لحماية التجارة الإلكترونية – ط1 – دار الفكر الجامعي – الإسكندرية – 2002م.
28. عصمت عبد المجيد بكر ود. صبري حمد خاطر – الحماية القانونية للملكية الفكرية – ط1 – بيت الحكمة – بغداد – 2001م.
29. عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة – (د.ت).
30. محمد الجبور – الجرائم الواقعة على أمن الدولة في القانون الأردني والقوانين العربية – ط2 – عمان – 2000م.
31. محمد الفاضل – التعاون الدولي في مكافحة الإجرام – بدون دار نشر – (د.ت).

32. محمد سامي الشوا – ثورة المعلومات وانعكاساتها على قانون العقوبات الجزء الثاني – دار النهضة العربية – القاهرة – 1994م.
33. محمد عبد الظاهر حسين – الاتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية – دار النهضة العربية – القاهرة – 2000/2001م.
34. محمد أحمد فكيرين – أساسيات الحاسب الآلي – دار الراتب الجامعية – بيروت – 1993م.
35. محمد عبد المحسن المقاطع – حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي – دراسة تحليلية نقدية مقارنة للحق في الخصوصية وتطبيقاته في القانون الكويتي – مطبوعات جامعة الكويت – الكويت – 1992م.
36. ذكي أمين حسونة– جرائم الكمبيوتر والجرائم الاخرى في مجال تكنولوجيا المعلومات، دار النهضة العربية القاهرة 1993.
37. ذياب البداينة، الأمن وحرب المعلومات دار الشروق عمان 2002.
38. عبد القادر عبدالله الفنتوخ، الانترنت للمستخدم العربي،مكتبة العبيكان، الرياض ط2، 2000.
a. محمد عبد الله منشاوي، "جرائم الإنترنت من منظور شرعي وقانوني،مكة المكرمة،1\11\2003 من خلال الموقع mohammed@minshawi.com
39. عبد الرحمن عبد العزيز الشنيفي حرب المعلومات مكتبة غريب الرياض 1991.
40. محمود السيد عبد المعطي الانترنت وبعض الجوانب القانونية، دار النهضة العربية القاهرة، 1998.
41. ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، 2004.
42. محمد محيي الدين عوضين، مشكلات السياسية الجنائية المعاصرة في جرائم نظم المعلومات، منشورات دار النهضة العربية، 1993.

43. نائل عبد الرحمن صالح/ واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط3، من 1–3 مايو 2000.

44. زياد عبد الكريم وآخرون، الكمبيوتر وتطبيقاته، دار المستقبل للنشر والتوزيع، عمان، 1990م.

45. علي حسن محمد طوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، جامعة عمان العربية للدراسات العليا، عمان، 2003.

46. رشا مصطفى أبو الغيط– الحماية القانونية للكيانات المنطقية، برامج الحاسوب، وصف البرامج المستندات الملحقة، ملتقى الفكر، الإسكندرية، 2000م .

47. محمد فهمي طلبة وآخرون، الموسوعة الشاملة لمصطلحات الحاسوب الإلكتروني، موسوعة دلتا كمبيوتر، مطابع المكتب المصري الحديث، القاهرة، 1991، ص 369.

48. محمد عبد الظاهر حسين، الاتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية، دار النهضة العربية، القاهرة، 2001/2000.

49. الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي، المؤرخة 2001/11/23، المادة (1/أ).

50. مقالة للعقيد محمد عبد الله منشاوي – باحث متخصص في دراسات جرائم الحاسوب والانترنت– مدير قسم الاحصاء والدراسات الجنائية.

51. سلام فارس تنورين، دراسة تم تقديمها في الجامعة اللبنانية، الفرع الفرنسي، الدراسات العليا– قانون الاعمال المحلي والدولي.

52. نائلة عادل محمد فريد قورة، جرائم الحاسبات الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية ، القاهرة، 2004.

53. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.

54. وليد العكوم، مفهوم وظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت ، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، ط 3، من 1-3 مايو 2000.

55. يوسف عراب، ورقة عمل – متطلبات ومخاطر الانفتاح الالكتروني من النواحي الفنية والتشريعية ، الاردن، 2003، www.arablow.org

56. يونس عرب، موسوعة القانون وتقنية المعلومات، دليل امن المعلومات والخصوصية- جرائم الكمبيوتر والانترنت، منشورات اتحاد المصارف العربية، الجزء الأول، ط1، 2002، ص299.

57. يونس عرب، "جرائم الكمبيوتر والإنترنت إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 2002\12\10.

58. يونس عرب، نظرية قانون الكمبيوتر، منشورات اتحاد المصارف العربية، 2001 من خلال الموقع: www.arablow.org.com

59. يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الامن العربي2002-تنظيم المركز العربي للدراسات والبحوث الجنائية- أبو ظبي 10-2002/2/12.

60. قانون العقوبات الاردني.

61. قانون المعاملات الالكترونية الاردني.

62. قانون الاتصالات.

63. قانون أصول المحاكمات الجزائية.

64. الموقع الالكتروني: www.ajeeb.com 2001/3/25.

65. علاء السالمي– المرجع السابق.

66. زياد القاضي وآخرون، تكمولوجيا المعلومات، ط1، كحلون، عمان، 1997.

67. ذياب البداينة، الأمن وحرب المعلومات.

68. محمود مصطفى، شرح قانون العقوبات، القسم الخاص – القاهرة 1984 – دار النهضة العربية.

69. حسن صادق المرصفاوي، قانون العقوبات الخاص – الإسكندرية – جلال حرى – سنة 1991.

70. محمود نجيب حسني، شرح قانون العقوبات القسم الخاص – القاهرة 1986.

71. عمر الفاروق الحسيني، لمحه عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، القانون والكمبيوتر والانترنت، المجلد الاول، ط3، 2004.

72. رؤف عبيد، جرائم الاعتداء على الأشخاص والأموال، الطبعة الثامنة، السنة 1985.

73. فوزية عبد الستار، شرح قانون العقوبات القسم الخاص – القاهرة – 1983.

74. هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، ط1، دار النهضة العربية، القاهرة، 1997.

75. هلالي عبد اللاه أحمد –حجية المخرجات الكمبيوترية في المواد الجنائية –دراسة مقارنة –أسيوط– 1999م.

76. فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت –لبنان، 2003.

77. حسن طاهر داود –جرائم نظم المعلومات –ط1 –أكاديمية نايف العربية للعلوم الأمنية –الرياض –2000م.

78. عبد الرحمن عبد العزيز الشنيفي، حرب المعلومات – الحرب القادمة.

79. محمد محيي الدين عوضين، مشكلات السياسية الجنائية المعاصرة في جرائم نظم المعلومات.

80. ذكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات.

81. محمد صبحي نجم، الوجيز في قانون أصول المحاكمات الجزائية، دار الثقافة– الاردن، ط1، 2006.

المراجع الأجنبية:

1. Report of the Attorney General's Task Force on Family Violence, U.S. Department of Justice, Washington, D. C.
2. Federal Bureau of Investigation, reported in "Talking Points: Important Facts About Pornography, Take Action Manual ,National Coalition for the protection of Children and Families, p. 8
3. Edward Donnerstein, "Pornography: Its Effects on Violence Against Women" in Malamuth and Donnerstein, eds., Pornography and Sexual Aggression, Academic Press, 1984
4. James Check, "The Effects of Violent and Nonviolent Pornography", Department of Justice, Ottawa Canada, submitted June 1984
5. Dolf Zillman and Jennings Bryant, "Pornography, Sexual Callousness, and the Trivialization of Rape, "Journal of Communications 32, 1982
6. Elizabeth Oddone Paolucci, Mark L. Genuis, and Claudio Violato, "The Effects of Pornography on Attitudes and Behaviours in Sexual and Intimate Relationships, "National Foundation for Family Research and Education (NFFRE), 2000
7. Testimony by John B. Rabun, deputy director, National Center for Missing and Exploited Children, before the subcommittee on Juvenile Justice of the Senate Judiciary Committee, 12 September 1984
8. Dr. Judith Reisman, the presiden of Washington's Institute for Media Education.
9. "American Drugs Culture Has Roots in Playboy. " National Federation for Decency Journal, November/Desember 1986
10. Kilpatrick et. Al. Rape in America:" A Report to the Nation, "April 23, 1992